ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ
ΥΠΟΛΟΓΙΣΤΩΝ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ:
ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ ΕΠΙΣΚΟΠΗΣΗ ΤΩΝ ΚΥΡΙΟΤΕΡΩΝ ΤΕΧΝΙΚΩΝ ΚΑΙ Ο ΑΝΤΙΚΤΥΠΟΣ ΣΤΗΝ ΚΟΙΝΩΝΙΑ

ΑΠΟΣΤΟΛΟΠΟΥΛΟΣ ΔΗΜΗΤΡΙΟΣ ΑΕΜ: 1701064 (135)

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΟΥΝΤΑΝΟΣ ΙΩΑΝΝΗΣ

Βόλος, Σεπτέμβριος 2011

Οπισθόφυλλο

ΠΕΡΙΛΗΨΗ

Πόσες φορές δεν έχετε ξεχάσει ή χάσει τα κλειδιά σας ή την κάρτα ανάληψης χρημάτων; Πόσες φορές έχετε ξεχάσει το PIN της δεύτερης πιστωτικής σας κάρτας ή το password για να έχετε πρόσβαση στον τρίτο σας λογαριασμό email; Δε θα ήταν πολύ πιο εύκολο να έχετε πρόσβαση σε εγκαταστάσεις ή υπηρεσίες απλά ακουμπώντας το δάκτυλο του χεριού σας σε ένα scanner ή να κοιτάζατε μια κάμερα? Αυτή την «ευκολία» προσφέρουν τα Βιομετρικά Συστήματα Αναγνώρισης. Τεχνολογίες δηλαδή που επιτρέπουν την αυθεντικοποίηση ενός χρήστη χρησιμοποιώντας κάτι που «είναι» και όχι κάτι που έχει ή γνωρίζει.

Το συγκεκριμένο θέμα πραγματεύεται η παρούσα διπλωματική, με τίτλο *Βιομετρικά Συστήματα Αναγνώρισης: Επισκόπηση των Κυριοτέρων Τεχνικών και ο Αντίκτυπος στην Κοινωνία.* Στην διπλωματική επισημαίνονται η έννοια του Βιομετρικού Συστήματος, οι τεχνολογίες που υπάρχουν και εφαρμόζονται, τα οφέλη από τη χρήση τέτοιων συστημάτων είτε είναι τεχνικής φύσεως είτε είναι οικονομικά ή κοινωνικά, αλλά και τα τις δυσκολίες που προκύπτουν στην εφαρμογή τους τόσο σε τεχνικό όσο και σε κοινωνικό επίπεδο.

ABSTRACT

How many times haven't you forgotten or have lost your keys or your ATM card? How many times haven't you forgotten your second credit card PIN or the password of your third email account? Wouldn't be easier to have access to facilities or applications simply by touching your finger on a scanner or by just facing a camera? Biometric Identification Systems provide this kind of ease. Technologies that allow a person's authentication using something that he/she "is" and not something he/she possesses or knows.

The present study, entitled Biometric Identification Systems: Overview of the Main Technologies and the Impact to Society, deals with this particular subject. This study highlights the meaning of a Biometric System, existing technologies and where are applied, technological, economical or social benefits, but also the difficulties that rise, during the application, in technological and social level.

Περιεχόμενα

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω όσους με βοήθησαν και μου συμπαραστάθηκαν κατά τη διάρκεια αυτής της επίπονης προσπάθειας. Ένα μεγάλο ευχαριστώ στους καθηγητές μου, που μου έδωσαν τα εφόδια για να αναπτυχθώ στην πανεπιστημιακή κοινότητα και να επιτύχω τους στόχους μου και ιδιαιτέρως στον κ. Σταμούλη Γεώργιο. Μεγάλο ευχαριστώ επίσης στους φίλους μου, χωρίς τους οποίους δε θα ήμουν ο άνθρωπος που είμαι τώρα. Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου, που όλα αυτά τα χρόνια μου συμπαραστέκονται ηθικά και οικονομικά και διαμορφώνουν γύρω μου ένα άνετο περιβάλλον, μέσα στο οποίο μπορώ να εργαστώ και να επεκτείνω τις γνώσεις μου.

ΕΙΣΑΓΩΓΗ

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα πληροφοριακά συστήματα. Η χρησιμοποίηση προχωρημένων τεχνολογιών προσφέρει πολλά πλεονεκτήματα, αλλά ταυτόχρονα αυξάνονται σημαντικά τα προβλήματα προστασίας και διαθεσιμότητας, Στην περίπτωση ενός ιατρικού πληροφοριακού συστήματος, για παράδειγμα, ο ασθενής θα πρέπει να είναι βέβαιος ότι τα προσωπικά του δεδομένα που δόθηκαν κατά την είσοδο στο νοσοκομείο ή αυτά που δημιουργήθηκαν κατά τη διάρκεια της νοσηλείας του, συλλέγονται, αποθηκεύονται και επεξεργάζονται, με τρόπο που αποκλείει λάθη και διατίθενται μόνο σε εξουσιοδοτημένους χρήστες. Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας (απόδοση, ποιότητα) για την εξασφάλιση της εύρυθμης λειτουργίας ενός οργανισμού.

Ο προσδιορισμός της ταυτότητας, ανεξάρτητα από τη μέθοδο, είναι ευρέως διαδεδομένος στην καθημερινότητά μας. Για παράδειγμα πρέπει συχνά να αποδεικνύουμε την ταυτότητά μας (αυθεντικοποίηση), για να έχουμε πρόσβαση σε τραπεζικούς λογαριασμούς, να πάρουμε χρήματα από ένα ATM, να κάνουμε login σε ένα υπολογιστή, να διεκδικήσουμε προνόμια από την πρόνοια, να περάσουμε σύνορα χωρών, να έχουμε φυσική πρόσβαση σε χώρους ασφαλείας και άλλα πολλά.

Ως συνήθως, προσδιορίζουμε την ταυτότητά μας και αποκτούμε πρόσβαση με το να χρησιμοποιούμε ταυτότητες, διαβατήρια, κλειδιά, σήματα, εμβλήματα, έξυπνες κάρτες πρόσβασης και προσωπικούς κωδικούς (PIN).Δυστυχώς, οι ταυτότητες, τα διαβατήρια, τα κλειδιά, τα σήματα, οι κάρτες είναι δυνατόν να χαθούν, να αντιγράφουν ή να κλαπούν. Όσο για τα passwords, τους μυστικούς κωδικούς και τα PINs είναι δυνατόν να ξεχαστούν εύκολα, να διαμοιραστούν ή να εκτεθούν. Τέτοιου είδους ανεπάρκειες στη συνηθισμένη προσωπική αναγνώριση ταυτότητας, έχουν προκαλέσει τεράστια προβλήματα.

Για να γίνει κατανοητό το μέγεθος του προβλήματος ας παραθέσουμε κάποια στοιχεία. Τα τελευταία 6 χρόνια γίνεται μια έρευνα στις Η.Π.Α. από το Ίδρυμα Ponemon. Στην έρευνα έως τώρα έχουν λάβει μέρος 593 επιχειρήσεις. Τα αποτελέσματα της έρευνας είναι αρκετά ανησυχητικά:

- Σχεδόν το 90% των εταιρειών που παίρνουν μέρος στην έρευνα έχουν αναφέρει τουλάχιστον ένα συμβάν ασφαλείας.

- Η εταιρεία Symantec και το Ίδρυμα Ponemon πρόσφατα αποκάλυψαν ότι το 59% των πρώην υπαλλήλων των εταιρειών παραδέχτηκαν ότι έκλεβαν δεδομένα από τους πρώην εργοδότες τους.
- Σύμφωνα με το Γραφείο εκκαθαρίσεως τραπεζικών επιταγών, 343.705.708 PII έχουν εκτεθεί από τη στιγμή που το ίδρυμα άρχισε την έρευνα.
- Σύμφωνα με την τραπεζική υπηρεσία έκδοσης καρτών, απατεώνες υπέκλεψαν περίπου 94 εκατομμύρια κάρτες.

Type of attack	2009	2010
Malware infection	50%	64%
Password sniffing	9%	17%
Financial fraud	12%	20%
Extortion or blackmail associated with release of stolen data	3%	7%
Exploit of user's social network profile	Option added in 2010	7%
Inside abuse of internet access (i.e. pornography, pirated software)	44%	30%
Unauthorized access	15%	24%
Physical unauthorized access	4%	9%
Theft of or unauthorized access to PII or PHI	13%	22%
System penetration by outsider	14%	18%
Being fraudulently represented as sender of phishing messages	31%	34%
Laptop or mobile hardware theft loss	42%	42%
Denial of service	21%	29%

Πίνακας 1. Είδη απειλών σύμφωνα με CSI/FBI Computer Crime and Security Survey Δείγμα 185 επιχειρήσεων

Φανταστείτε ότι κάποιος θέλει να ενημερωθεί για τα e-mail του από κάποιον υπολογιστή και πρέπει να κάνει log in. “Παρακαλώ τοποθετήστε το δείκτη του δεξιού χεριού σας στον αναγνώστη δακτυλικών αποτυπωμάτων” αναφέρει ένα μήνυμα στην οθόνη του υπολογιστή. Ο χρήστης το κάνει και μετά στην οθόνη εμφανίζεται “WELCOME”.

Ευκολία και ασφάλεια συνδυάζονται για να παραχωρήσουν πρόσβαση σε μια υπηρεσία, σε εξουσιοδοτημένους χρήστες και ταυτόχρονά να αποτρέψουν την μη εξουσιοδοτημένη πρόσβαση σε αυτή. Δεν υπάρχει η ανάγκη για να θυμόμαστε passwords και έτσι εξαλείφεται και ο φόβος απώλειάς τους. Μείωση λοιπόν στα λάθη, στις απάτες και στις επιπτώσεις αυτών, μέσω ισχυρότερης εμπιστοσύνης στην διαδικασία της αυθεντικοποίησης. Αυτό, με λίγα λόγια, είναι εκείνο που υπόσχονται ότι θα προσφέρουν στη διαδικασία της αυθεντικοποίησης και του προσδιορισμού της ταυτότητας τα συστήματα βιομετρικής αναγνώρισης.

Η χρήση των συστημάτων βιομετρικής αναγνώρισης θα αυξηθεί σημαντικά στο μέλλον. Ένας από τους λόγους είναι ότι σε μια κοινωνία στην οποία οι ηλεκτρονικοί υπολογιστές αποτελούν, όλο και περισσότερο, μέρος της καθημερινότητάς μας και αναπόσπαστό κομμάτι στην εργασία και στην κάθε είδους τεχνολογική πρόοδο, είναι επιτακτική η ανάγκη για τη χρήση πιο αποτελεσματικών συστημάτων αυθεντικοποίησης. Επίσης οι εγκληματίες έχουν πλέον βρει τόπους να παρακάμψουν τα παλιά συστήματα αυθεντικοποίησης. Επιπρόσθετα, καθώς τα βιομετρικά συστήματα θα γίνονται καλύτερα, φθηνότερα και πιο αξιόπιστα, σταδιακά θα εφαρμοστούν και σε άλλα περιβάλλοντα, όπως στα σπίτια, στα σχολεία, στην εργασία. Αυτό είναι το “φαινόμενο της διάχυσης”.

Το πλεονέκτημα που παρέχει η βιομετρική αυθεντικοποίηση είναι η δυνατότητα να απαιτούμε περισσότερες φάσεις αυθεντικοποίησης σε απλό και γρήγορο τρόπο έτσι ώστε ο χρήστης να μην ενοχληθεί από επιπρόσθετες απαιτήσεις του συστήματος. Για παράδειγμα την απομακρυσμένη επικοινωνία με τη σχολή. Όνομα χρήστη και password για να αποκτήσεις πρόσβαση στο λογαριασμό email, όνομα χρήστη και password για πρόσβαση στο site της σχολής, όνομα χρήστη και password για την πρόσβαση στο σύστημα της e-γραμματείας, όνομα χρήστη και password για πρόσβαση στο e-class. Ο σχεδιαστής έχει σχεδιάσει έτσι το σύστημα για να έχει ένα αποδεκτό επίπεδο ασφαλείας που ορίζεται στην ανάλυση επικινδυνότητας (risk assessment) του πληροφοριακού συστήματος. Πόσο πιο απλό θα ήταν κάθε φορά αντί για πληκτρολόγηση ο χρήστης να ακουμπά τον αντίχειρά του σε ένα scanner;

Πρακτικά, τα βιομετρικά συστήματα θα χρησιμοποιούνται κυρίως για τρεις λόγους: επιβολή του νόμου (law enforcement), έλεγχος φυσικής πρόσβασης (physical access control) συμπεριλαμβανομένου και του ελέγχου στα σύνορα και έλεγχος λογικής πρόσβασης (logical access control).

Πολλοί άνθρωποι έχουν συνδυάσει τη βιομετρία με τους εγκληματίες και για αυτό το λόγο δείχνουν δυσπιστία απέναντι σε τέτοιου είδους συστήματα. Η επιβολή του νόμου όμως, αποτελεί μέχρι τώρα τη μόνη περιοχή στην οποία εφαρμόζονται μεγάλης κλίμακας βιομετρικές εφαρμογές εδώ και πολύ καιρό.

Ο έλεγχος φυσικής πρόσβασης βασισμένος στη βιομετρία, έως τώρα έχει χρησιμοποιηθεί μόνο σε περιορισμένη κλίμακα, κυρίως σε εταιρίες. Όμως υπάρχουν αρκετά δοκιμαστικά ή προσφάτως ολοκληρωμένα προγράμματα, τα περισσότερα εκ των οποίων στα αεροδρόμια, τα οποία έχουν δοκιμάσει βιομετρικό έλεγχο σε μεγάλο αριθμό επιβατών χωρίς την αρωγή προσωπικού. Το πιο σημαντικό, από την πλευρά της πολιτείας, η διείσδυση των βιομετρικών στα διαβατήρια θα δημιουργήσει για πρώτη φορά μια μεγάλης κλίμακας εφαρμογή ελέγχου φυσικής πρόσβασης.

Η χρήση των βιομετρικών συστημάτων στον έλεγχο της λογικής πρόσβασης, κυρίως στις διαδικτυακές ταυτότητες, προβλέπεται ότι θα σημειώσει ραγδαία αύξηση. Πραγματοποιούνται όλο και περισσότερες διαδικτυακές συναλλαγές, όπως e-banking, e-commerce, e-shopping, e-government και τα βιομετρικά προσφέρουν έναν πολλά υποσχόμενο τρόπο διαμόρφωσης ασφαλών ταυτοτήτων, ειδικά όταν η κατά πρόσωπο επαφή δεν είναι εφικτή. Αυτό είναι ιδιαίτερα σημαντικό για υψηλής αξίας οικονομικές δοσοληψίες και για την μετάδοση εμπιστευτικών δεδομένων.

Ο διαχωρισμός αυτός στη θεωρία μας διευκολύνει αρκετά στην ανάλυση, όμως πρακτικά οι λόγοι αυτοί συνδυάζονται μεταξύ τους. Για παράδειγμα σε ένα σωφρονιστικό ίδρυμα μπορεί να συνδυαστεί έλεγχος φυσικής πρόσβασης για πρόσβαση στο κτήριο μαζί με έλεγχο λογικής πρόσβασης για την ανάκτηση δεδομένων κάποιων κρατουμένων.

Έρευνες που αφορούν την ανθρώπινη μνήμη, έχουν δείξει ότι κάποιος θυμάται ένα αντικείμενο πιο εύκολα όταν καλείται να το παράξει ο ίδιος, παρά όταν πρέπει να το διαβάσει και να το απομνημονεύσει. Έτσι αν οι χρήστες έχουν τη δυνατότητα να παράγουν τα δικά τους passwords θα τα θυμούνται και πιο εύκολα. Το μειονέκτημα όμως είναι ότι δεν μπορούν να θυμηθούν “δυνατά” passwords και ταυτόχρονα τα passwords που μπορούν να θυμούνται είναι εύκολο κάποιος να τα μαντέψει. Η ικανότητα ανάκλησης αντικειμένων από τη μνήμη, εξαρτάται από το φόρτο της

μνήμης (memory load), δηλαδή από των αριθμό των αντικειμένων που έχουμε στη μνήμη μας. Όσο ο φόρτος της μνήμης αυξάνεται, ο αριθμός των αντικειμένων που ξεχνάμε αυξάνεται (Ian Neath,1998). Συνεπώς, όσο περισσότερα passwords πρέπει να θυμόμαστε, τόσο μειώνεται η πιθανότητα ανάκλησης ενός συγκεκριμένου password. Η ραγδαία ανάπτυξη των e-υπηρεσιών έχουν κάνει τα προβλήματα του φόρτου της μνήμης πιο εμφανή, γιατί οι χρήστες πρέπει να παράγουν passwords τα οποία ικανοποιούν ποικίλα κριτήρια. Για παράδειγμα κάποια Web sites δεν έχουν περιορισμούς στα passwords, ενώ κάποια άλλα απαιτούν να χρησιμοποιηθούν αλφαριθμητικά συγκεκριμένου μήκους ή να συνδυάζουν γράμματα και αριθμούς. Έρευνα που έγινε από τις εταιρείες Safe Net και RSA Security έδειξε ότι σε δείγμα 3050 χρηστών του διαδικτύου, το 55% αναγκάζεται να γράφει κάπου τα passwords και το 50% των χρηστών ζητούσαν να γίνει reset το password γιατί το ξέχασαν. Υπολογίστηκε ότι κάθε reset password που γινόταν κόστιζε περίπου 25-50.

Στα πλαίσια της συγκέντρωσης στοιχείων έκρινα σκόπιμο να κάνω μια έρευνα που έχει να κάνει με χρήση των ηλεκτρονικών υπηρεσιών και τη χρήση passwords. Ολόκληρη η έρευνα βρίσκεται στο ΠΑΡΑΡΤΗΜΑ Α. Τα αποτελέσματα όσον αφορά το θέμα της ασφάλειας δεν είναι και τόσο ενθαρρυντικά. Παραθέτω ένα μικρό παράδειγμα. Το 57% των ερωτηθέντων χρησιμοποιεί το ίδιο password για κάθε υπηρεσία που χρησιμοποιεί. Το πιο ανησυχητικό όμως είναι ότι το 68% έχει κάποιο backup για τα passwords που χρησιμοποιεί. Μάλιστα από το 43% των ερωτηθέντων που χρησιμοποιούν διαφορετικά passwords, το 92% έχει κάποιο backup.

ΚΕΦΑΛΑΙΟ 1: ΒΑΣΙΚΕΣ ΒΙΟΜΕΤΡΙΚΕΣ ΕΝΝΟΙΕΣ

Η **Βιομετρία** χρησιμοποιεί τεχνικές αναγνώρισης προτύπων προς προσδιορισμό της ταυτότητας των χρηστών μέσα από σωματικά χαρακτηριστικά ή χαρακτηριστικά συμπεριφοράς.

Ιστορική αναδρομή

Οι Άγγλοι είχαν αρχίσει να χρησιμοποιούν τα δακτυλικά αποτυπώματα για αυθεντικοποίηση από τον Ιούλιο του 1858, όταν πρώτος ο Σερ William James

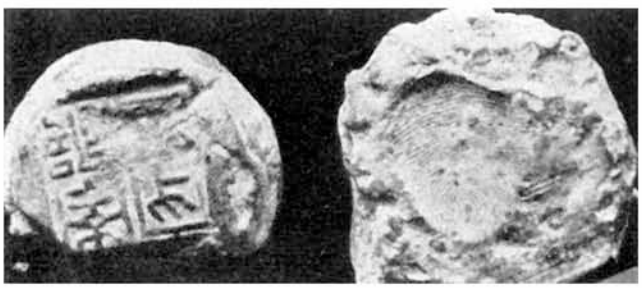
Herschel, ένας πταισματοδίκης στο Jungipoor της Ινδίας, χρησιμοποίησε το αποτύπωμα της παλάμης του σε ένα συμβόλαιο. Οι ντόπιοι ενθουσιάστηκαν και έγινε συνήθης πρακτική να επικυρώνεται ένα συμβόλαιο με το αποτύπωμα της παλάμης για να αποφευχθεί η παραχάραξη.

KONAI's HANDPRINT
from the back of the contract
Bengal, India, 1858

Contract for 2,000 maunds (165,200 Lbs.) of road-metalling,
between W.J. Herschel and Rajyadhar Konai, in Konai's handwriting

Εικόνα 1. Επικυρωμένο συμβόλαιο με το αποτύπωμα του χεριού

Τη δεκαετία του 1870, ο Δρ. Henry Faulds, Βρετανός χειρούργος στο νοσοκομείο Tsukiji του Τόκυο, άρχισε να ασχολείται με τα "αυλάκια του δέρματος", όταν ανακάλυψε ίχνη από δακτυλικά αποτυπώματα σε προϊστορικά κεραμικά. Ο Δρ. Faulds όχι μόνο αναγνώρισε τη σπουδαιότητα των αποτυπωμάτων, αλλά σχεδίασε και μια μέθοδο κατάταξης. Το 1880 έστειλε τη μελέτη του στον Κάρολο Δαρβίνο, αλλά εξαιτίας της προχωρημένης ηλικίας του ο Δαρβίνος δεν μπορούσε να τον βοηθήσει και δεσμεύτηκε να την προωθήσει στον ξάδερφό του Francis Galton.



Εικόνα 2. Ίχνη από δακτυλικά αποτυπώματα σε προϊστορικάκεραμικά

Την ίδια χρονιά ο Δρ. Faulds δημοσίευσε ένα άρθρο στο επιστημονικό περιοδικό *Nature*. Συζητούσε για τα δακτυλικά αποτυπώματα ως μέσω αναγνώρισης και τη χρήση του μελανιού ως μέθοδο λήψης αυτών. Πιστώνεται επίσης την πρώτη αναγνώριση δακτυλικού αποτυπώματος πάνω σε ένα λαδωμένο μπουκάλι αλκοόλ.

Μια νέα μέθοδος αναγνώρισης της ταυτότητας ενός ατόμου, έρχεται στο προσκήνιο τη 1882, από τον Alphonse Bertillon, έναν υπάλληλο στην αστυνομία του Παρισιού. Το 1888 γίνεται αρχηγός του νεοσυσταθέντος Τμήματος Δικαστικής Αυθεντικοποίησης, όπου χρησιμοποιούσε το ανθρωπομετρικό του σύστημα ως κύριο μέσο για την αναγνώριση. Το ανθρωπομετρικό σύστημα αναγνώρισης του, βασιζόταν στα εξής :

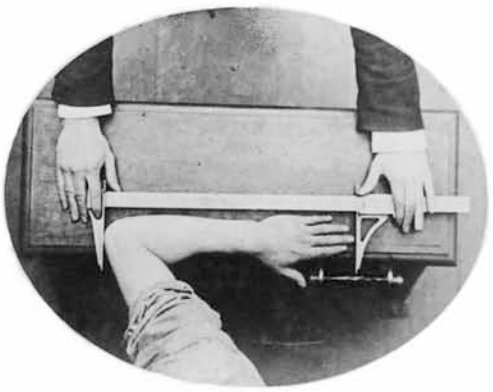
1) Διαφορετικές μετρήσεις, από ειδικά σχεδιασμένα όργανα.
2) Ακριβής φυσική περιγραφή.
3) Καταγράφονται «ασυνήθιστα σημάδια».

Η μέθοδος όμως του Bertillon δεν ήταν αλάνθαστη. Τα μειονεκτήματα της μεθόδου ήταν πολύ συγκεκριμένα και πολύ δύσκολο να αγνοηθούν:

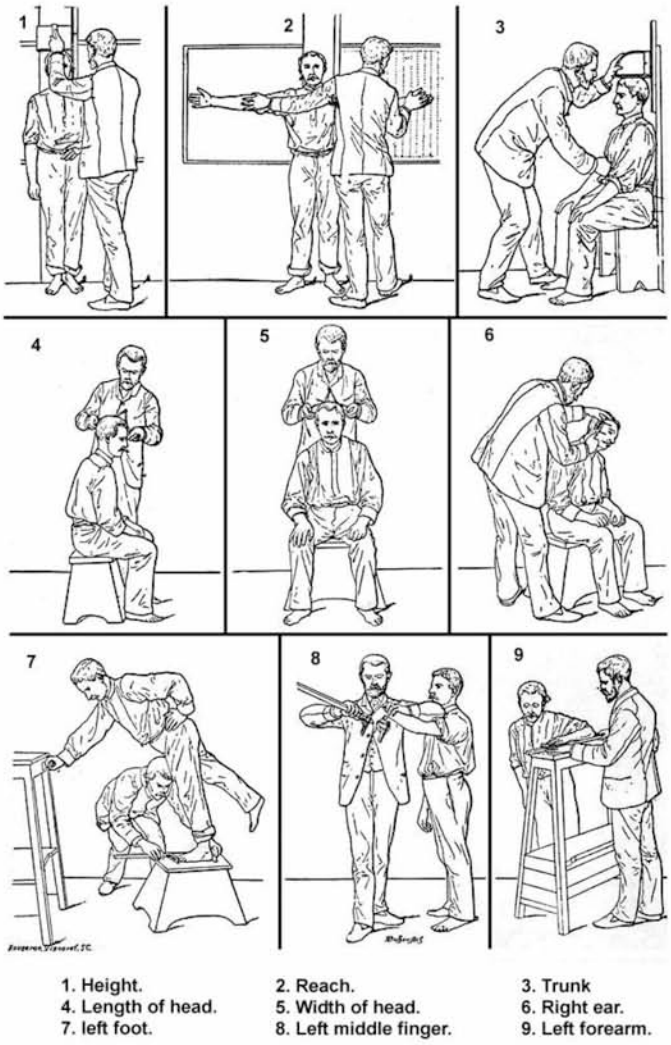
1. Πολύπλοκο σύστημα καταγραφής

   -Εξειδικευμένοι χειριστές των οργάνων, επόπτες και ειδικός (ακριβός) εξοπλισμός χρειαζόταν για ακρίβεια στις μετρήσεις.

2. Υψηλά ποσοστά σφάλματος.

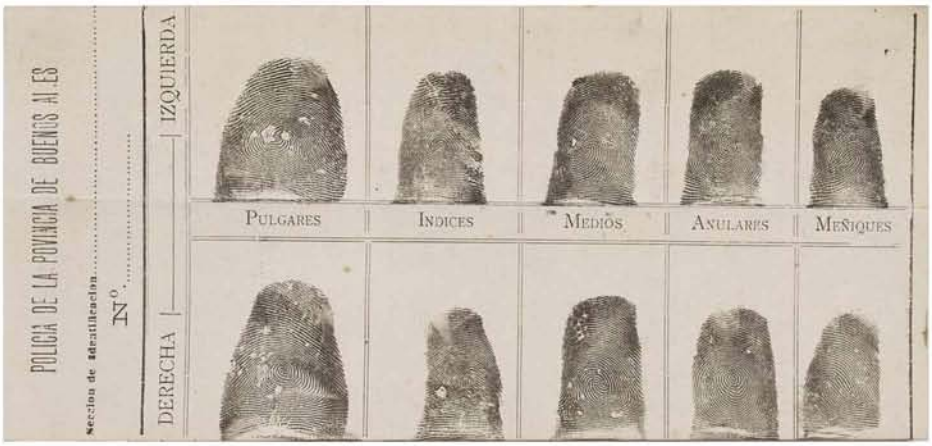


Εικόνες 3 και 4. Μέτρηση απόστασης αγκώνα-μέσου



Εικόνα 5.Βιομετρικές τεχνικές του παρελθόντος

Συνεχίζοντας την ιστορική αναδρομή, η πιο παλιά μέθοδος και εκείνη με τη μεγαλύτερη εξέλιξη, είναι η αναγνώριση των αποτυπωμάτων. Το 1892 ο Francis Galton, Βρετανός ανθρωπολόγος εκδίδει το *Finger Prints,* μια μελέτη για τη χρησιμοποίηση δακτυλικών αποτυπωμάτων ως μέσω αναγνώρισης, δίνοντας έμφαση στη μοναδικότητα και στη μονιμότητα των δακτυλικών αποτυπωμάτων. Ο Juan Vucetich, ένας αστυνόμος από την Αργεντινή χρησιμοποιώντας την μελέτη του Francis Galton έκανε την πρώτη χρήση ταυτοποίησης με δακτυλικά αποτυπώματα για την εξιχνίαση ενός εγκλήματος. Μια γυναίκα, η Francis Rojas, αφού σκότωσε τους δυο γιους της, αυτοκτόνησε για να ενοχοποιήσει κάποιον άλλον. Κατάφερε να τη αναγνωρίσει από ένα ματωμένο αποτύπωμά της στην κάσα της πόρτας.



Εικόνα 6. Δακτυλικά αποτυπώματα

Το 1894 ο Marc Twain εκδίδει τη νουβέλα, *Pudd'nhead Wilson,* μια νουβέλα στην οποία ένας δικηγόρος, ο David Wilson, καταφέρνει να λύσει μια υπόθεση δολοφονίας, χάρις το χόμπι του να συλλέγει δακτυλικά αποτυπώματα. Το 1902 ο Edward Henry της Scotland Yard χρησιμοποιεί αποτυπώματα για να αποδειχθεί η ενοχή κάποιου στη Βρετανία. Το 1905 ο Αμερικανικός στρατός αρχίζει να χρησιμοποιεί δακτυλικά αποτυπώματα, ενώ την ίδια χρονιά το αμερικανικό υπουργείο δικαιοσύνης δημιουργεί την υπηρεσία Αναγνώρισης Εγκλημάτων, στην Ουάσιγκτον, για να υπάρχουν συγκεντρωμένες συλλογές αποτυπωμάτων. Το 1924 το κογκρέσο ιδρύει το τμήμα αναγνώρισης του FBI. Μέχρι το 2005 η Interpol είχε στην κατοχή της 50.000 αποτυπώματα εγκληματιών και το 2009 το σύστημα AFIS (Automated Fingerprint Identification System) της αμερικανικής εθνικής ασφάλειας, μετρά πάνω από 100 εκατομμύρια δακτυλικά αποτυπώματα.

Ορισμοί

Βιομετρικό είναι ένα μετρήσιμο φυσικό χαρακτηριστικό ή ένα προσωπικό συμπεριφορικό γνώρισμα, το οποίο χρησιμοποιείται για την αναγνώριση της ταυτότητας ή την επαλήθευση της ταυτότητας που κάποιος χρήστης ισχυρίζεται πως έχει. Παραδείγματα φυσικών βιομετρικών είναι το σχήμα της παλάμης, τα δακτυλικά αποτυπώματα, η ίριδα, ο αμφιβληστροειδής, η γεωμετρία του προσώπου. Συμπεριφορικά γνωρίσματα είναι η φωνή, η υπογραφή, ο τρόπος που πληκτρολογούμε μια λέξη, ακόμη και ο τρόπος που περπατάμε.

Ένα **βιομετρικό σύστημα** είναι ένα αυτόματο σύστημα ικανό να :

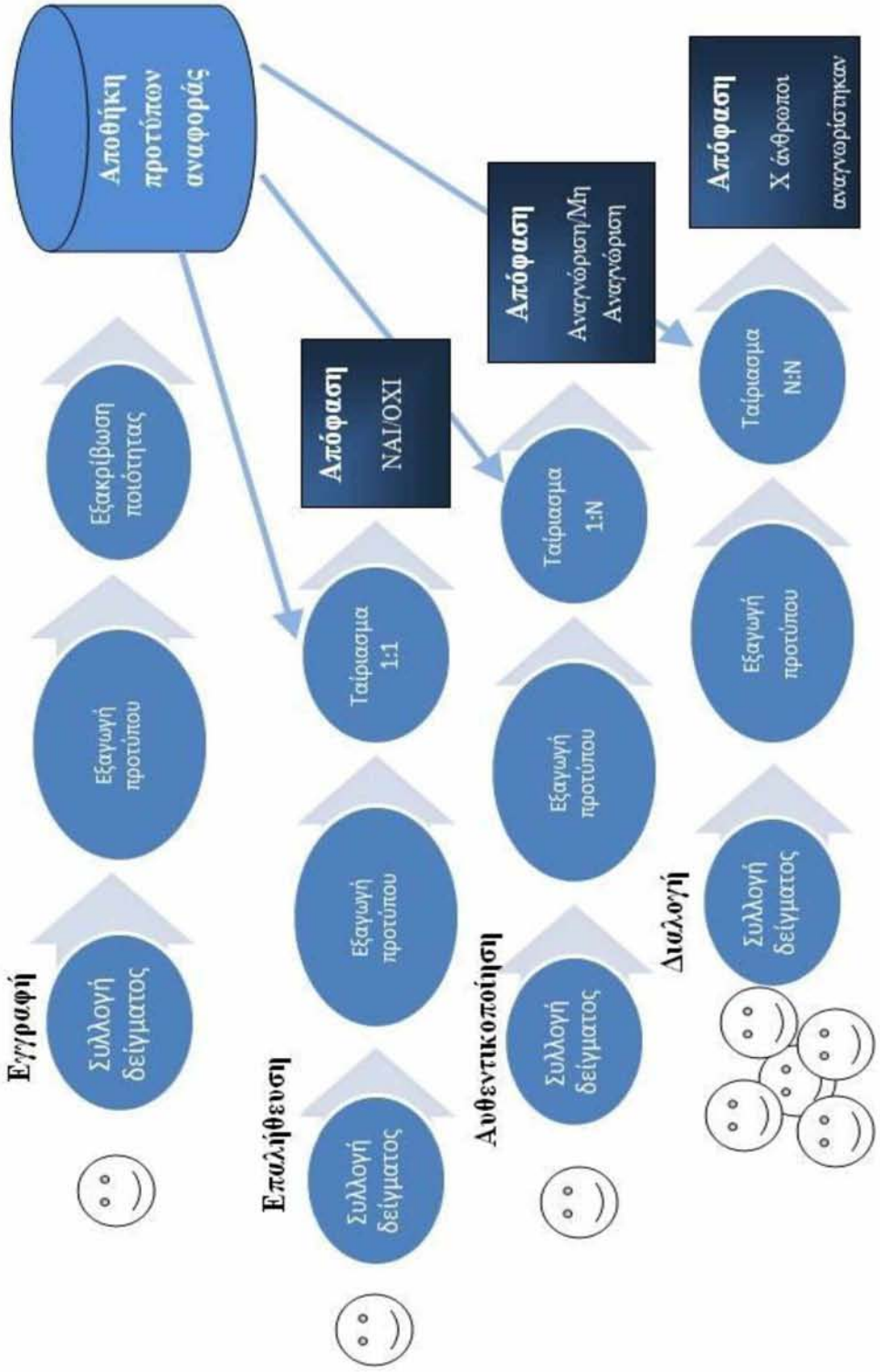
1) συλλέξει ένα βιομετρικό δείγμα από ένα χρήστη.
2) εξάγει βιομετρικά δεδομένα / πρότυπα από το συγκεκριμένο δείγμα.
3) συγκρίνει τα βιομετρικά δεδομένα / πρότυπα με εκείνα που περιέχονται στη βάση δεδομένων του.
4) αποφασίζει το βαθμό ομοιότητας των βιομετρικών δεδομένων / προτύπων.
5) δείξει αν επιτεύχθηκε ή όχι ο προσδιορισμός ή η επαλήθευση της ταυτότητας.

Η ανάγκη για αναγνώριση των χρηστών προήλθε από την επιθυμία ελέγχου πρόσβασης σε υπολογιστές και στον περιορισμό πρόσβασης ατόμων σε κτήρια ή προστατευμένες περιοχές. Έπρεπε λοιπόν να αναπτυχθούν τεχνικές όχι μόνο για την **αναγνώριση** των χρηστών, αλλά και για την **αυθεντικοποίηση** τους, να επιβεβαιωθεί δηλαδή ότι κάποιος είναι πράγματι το πρόσωπο που ισχυρίζεται ότι είναι. Αυθεντικοποίηση καλείται η διαδικασία επιβεβαίωσης της ταυτότητας ενός χρήστη. Το σύστημα αυθεντικοποίησης αποτελεί την πρώτη γραμμή άμυνας, αποσκοπώντας στο να αποτρέψει μη εξουσιοδοτημένους χρήστες να επιτύχουν πρόσβαση στο υπολογιστικό σύστημα. Μέσω τριων τεχνικών είναι εφικτή η αυθεντικοποίηση ενός προσώπου:

1) Αυθεντικοποίηση από κάτι **που γνωρίζει** (πχ. Password ή PIN)
2) Αυθεντικοποίηση από κάτι **που κατέχει** (πχ. Smart card)
3) Αυθεντικοποίηση από κάτι **που είναι** ο χρήστης (πχ. Βιομετρικά, υπογραφή)

Η βιομετρική αυθεντικοποίηση αποτελείται από τέσσερα στάδια : την εγγραφή (enrolment), την αποθήκευση (storage), την ανάκτηση (acquisition) και το ταίριασμα (matching). Αρχικά, ο χρήστης εγγράφεται, δημιουργείται δηλαδή μια εγγραφή που αντιστοιχεί το χαρακτηριστικό αναγνώρισης με τον χρήστη. Για παράδειγμα, πραγματοποιείται μια αναγνώριση δακτυλικού αποτυπώματος και το αποτέλεσμα τιτλοφορείται ως “Γιώργος Παπαδόπουλος”. Στη συνέχεια, ένα αντίγραφο αυτής της εγγραφής αποθηκεύεται κάπου. Υπάρχουν δυο επιλογές αποθήκευσης : οι εγγραφές αποθηκεύονται σε μια κεντρική βάση δεδομένων ή χρησιμοποιείται ένα πιο αποκεντρωτικό μοντέλο, όπως αποθήκευση σε smart cards. Έπειτα, όταν ζητηθεί να γίνει αυθεντικοποίηση, γίνεται μια νέα ανίχνευση (scan), δηλαδή μια καινούρια αναγνώριση δακτυλικού αποτυπώματος. Τέλος, η νέα εγγραφή συγκρίνεται με την

αποθηκευμένη εγγραφή. Αν ταιριάζουν, ο χρήστης έχει αναγνωριστεί-αυθεντικοποιηθεί.



Εικόνα 7. Βιομετρική διαδικασία

Κριτήρια αξιολόγησης

Οι πιο διαδεδομένες τεχνικές βιομετρικής αυθεντικοποίησης είναι η αναγνώριση δακτυλικού αποτυπώματος, η αναγνώριση προσώπου, η αναγνώριση ίριδας και η εξέλιξή της, η αναγνώριση αμφιβληστροειδούς και το DNA. Για να αναλύσουμε αυτές τις τεχνικές και πολύ περισσότερο για να τις συγκρίνουμε θα πρέπει να έχουμε κάποια κριτήρια. Υπάρχουν λοιπόν επτά κριτήρια τα οποία χρησιμοποιούμε για να αξιολογήσουμε ένα βιομετρικό χαρακτηριστικό και κατ' επέκταση την τεχνική αναγνώρισης.

1. Καθολικότητα (Universality) : Όλοι οι άνθρωποι έχουν κληροδοτηθεί με τα ίδια φυσικά χαρακτηριστικά. Ένα χαρακτηριστικό για να χρησιμοποιηθεί ως βιομετρικό θα πρέπει να το έχουν όλοι ή εκείνοι που δεν το έχουν δεν θα πρέπει να ξεπερνάνε το 1% του πληθυσμού.
2. Μοναδικότητα (Uniqueness) : Για κάθε άνθρωπο κάποια χαρακτηριστικά είναι μοναδικά. Υπάρχει βέβαια και η περίπτωση των πανομοιότυπων διδύμων τα οποία πιθανόν να έχουν πολλά κοινά χαρακτηριστικά.
3. Μονιμότητα (Permanence) : Τα χαρακτηριστικά δεν αλλοιώνονται από το χρόνο. Ο βαθμός μονιμότητας επηρεάζει σημαντικά στο σχεδιασμό του συστήματος.
4. Ικανότητα Συλλογής (Collectability) : Τα μοναδικά χαρακτηριστικά ενός ατόμου πρέπει να συλλέγονται με έναν εύκολο, σε λογικά πλαίσια, τρόπο. Πρακτικά η συλλογή θα πρέπει να γίνεται αξιόπιστα, με ένα μη ενοχλητικό τρόπο και να κοστίζει ανάλογα με τη δεδομένη εφαρμογή.
5. Απόδοση (Performance) : Ο βαθμός ακρίβειας αυθεντικοποίησης πρέπει να είναι αρκετά υψηλός προτού το σύστημα τεθεί σε λειτουργία.
6. Αποδοχή (Acceptability) : Ο βαθμός αποδοχής μιας εφαρμογής. Οι εφαρμογές δεν θα είναι επιτυχημένες αν το κοινό αντιστέκεται στη χρησιμοποίησή τους.
7. Ανθεκτικότητα στην παράκαμψη (Resistance to circumvention) : Ένα βιομετρικό σύστημα θα πρέπει να είναι δύσκολο να παρακαμφθεί.

Όμως θα πρέπει να έχουμε κατά νου, ότι ο βαθμός εκπλήρωσης κάθε κριτηρίου εξαρτάται από το είδος της εφαρμογής. Ο συνοριακός έλεγχος θα πρέπει να γίνεται γρήγορα, ενώ μια εγκληματολογική μελέτη μπορεί να διαρκέσει ακόμη και βδομάδες. Σε μια εφαρμογή, για παράδειγμα, διοδίων θα πρέπει να είναι αποδεκτό ένα μεγάλο

ποσοστό λάθους, ενώ σε μια τραπεζική εφαρμογή το ποσοστό αυτό θα πρέπει να είναι όσο το δυνατό χαμηλότερο. Ένα από τα πιο σημαντικά χαρακτηριστικά είναι το κατά πόσο ένα βιομετρικό είναι φιλικό προς τον χρήστη (user friendly). Η διαδικασία θα πρέπει να είναι απλή και γρήγορη, για παράδειγμα η λήψη μιας φωτογραφίας, το να μιλήσει ο χρήστης σε ένα μικρόφωνο ή ακουμπήσει με το δάκτυλό του ένα scanner.

Αρχιτεκτονική και διαδικασίες

Η αρχιτεκτονική ενός βιομετρικού συστήματος.

— Συλλογή δείγματος (Sample acquisition) : Αρχικά η λήψη των βιομετρικών δεδομένων πρέπει να γίνει χρησιμοποιώντας τον κατάλληλο σένσορα.

— Εξαγωγή προτύπου (Feature extraction) : Σε αυτό το βήμα μετατρέπεται το δείγμα σε πρότυπο. Το πρότυπο είναι αριθμητικά δεδομένα.

— Εξακρίβωση ποιότητας (Quality verification) : Επαναλαμβανόμενη συλλογή δείγματος και εξαγωγή προτύπου έως ότου εξασφαλιστεί ότι το σύστημα έχει συλλάβει και αναγνωρίσει τα δεδομένα σωστά.

— Αποθήκευση προτύπου αναφοράς (Storage of reference template) : Αποθηκεύεται το πρότυπο σε διαφορετικών ειδών μονάδες αποθήκευσης, από μια smartcard έως ένα server.

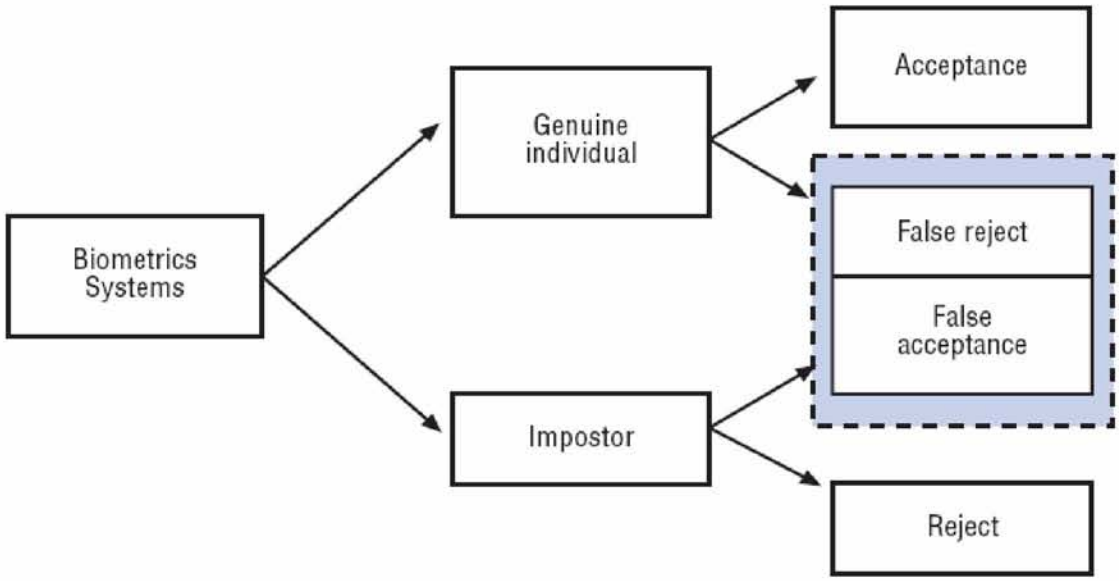
— Ταίριασμα (Matching) : Σε αυτό το βήμα συγκρίνεται το πρότυπο που εξάγεται εκείνη τη στιγμή με το αποθηκευμένο πρότυπο.

— Απόφαση (Decision) : Εδώ χρησιμοποιείται το αποτέλεσμα του ταιριάσματος για να βγει ένα αποτέλεσμα, σύμφωνα με κάποια κριτήρια που εξαρτώνται από την εφαρμογή.

Η διαδικασία της εγγραφής, η οποία αποτελεί το πρώτο βήμα κάθε βιομετρικού συστήματος, αποτελείται από τη συλλογή του βιομετρικού δείγματος, την επεξεργασία των βιομετρικών δεδομένων έτσι ώστε να αποσπάσουμε το δείγμα αναφοράς και την αποθήκευσή του για περαιτέρω χρήση. Η αποτελεσματικότητα και η ακρίβεια ενός βιομετρικού συστήματος, εξαρτάται άμεσα από τη διαδικασία της εγγραφής. Κατά τη διάρκεια του κύκλου ζωής ενός βιομετρικού, κάποιες φορές είναι αναγκαία η επανεγγραφή, λαμβάνοντας υπόψη τη φυσική αλλά και τη αναπάντεχη εξέλιξη/αλλαγή των βιομετρικών χαρακτηριστικών. Για παράδειγμα πρέπει να

υπολογίσουμε τη γήρανση του προσώπου, την αλλαγή φωνής, κάποια ασθένεια στα μάτια, ακόμη και κάποιο πιθανό τραυματισμό στο χέρι.

Η αυθεντικοποίηση είναι μια στατιστική διαδικασία. Η ποικιλία στις συνθήκες μεταξύ εγγραφής και ανάκτησης, καθώς και οι σωματικές αλλαγές δεν επιτρέπουν ένα 100% ταίριασμα. Για τα password ή τα PIN , η απάντηση που δίνεται είναι είτε ακριβώς η ίδια με την αποθηκευμένη είτε όχι. Ακόμη και η παραμικρή απόκλιση αποτελεί λόγο για αποτυχία. Για ένα βιομετρικό, δεν υπάρχει σαφής διαχωρισμός ανάμεσα σε ένα ταίριασμα ή σε μια αποτυχία. Συνεπώς η ύπαρξη ενός επιτυχούς ταιριάσματος εξαρτάται όχι μόνο από τα δυο σετ δεδομένων που συγκρίνονται, αλλά και από το περιθώριο λάθους το οποίο είναι ανεκτό. Μια πιθανότητα της τάξης του 95% μπορεί να θεωρείται ή όχι αποδεκτή, ανάλογα με την υλοποίηση του βιομετρικού συστήματος και τις απαιτήσεις ασφαλείας που καθορίζει η πολιτική ασφαλείας του εκάστοτε οργανισμού ή εταιρίας. Σαν συνέπεια αυτού, τα βιομετρικά συστήματα δεν μπορούν ποτέ να είναι 100% ακριβή.



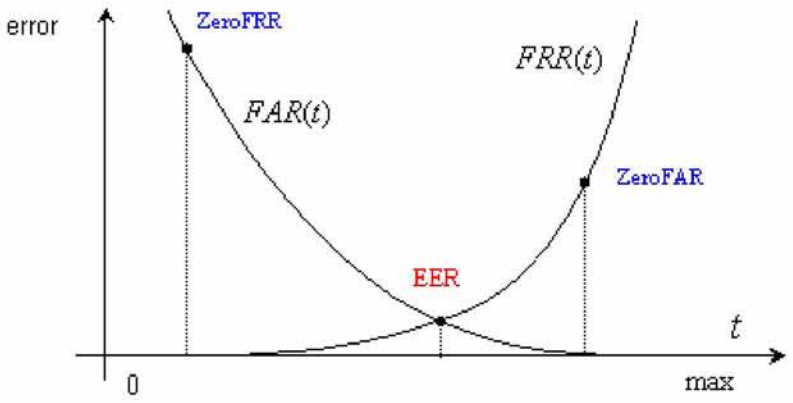
Εικόνα 8. Η βιομετρική διαδικασία

Υπάρχουν δυο ειδών πιθανά λάθη: λανθασμένο ταίριασμα (false acceptance) και λανθασμένη αποτυχία ταιριάσματος (false rejection). Ένα λανθασμένο ταίριασμα προκύπτει όταν ένα βιομετρικό πρότυπο (templates) ταιριάζεται λανθασμένα με ένα πρότυπο που βρίσκεται αποθηκευμένο, παρόλο που τα δυο πρότυπα ανήκουν σε διαφορετικούς ανθρώπους. Μια λανθασμένη αποτυχία ταιριάσματος προκύπτει όταν

ένα πρότυπο δεν κρίνεται ικανό να ταιριάξει με ένα αποθηκευμένο πρότυπο, παρόλο που τα δυο πρότυπα προέρχονται από το ίδιο άτομο. Δυο βιομετρικά πρότυπα που ανήκουν στο ίδιο άτομο και λήφθηκαν διαφορετικές χρονικές στιγμές, είναι δυνατόν να διαφέρουν εξαιτίας των περιβαλλοντολογικών αλλαγών, της διαφορετικής τοποθέτησης του οργάνου στον αισθητήρα ή κάποιου θορύβου. Εξαιτίας αυτού, το ταίριασμα γίνεται μέσω ενός αλγορίθμου ο οποίος υπολογίζει ένα ποσοστό ομοιότητας και το συγκρίνει με ένα αποδεκτό κατώφλι. Αν το ποσοστό ομοιότητας είναι τουλάχιστον ίσο με το κατώφλι, τότε το σύστημα αποκρίνεται ότι υπάρχει ταίριασμα. Όπως αναφέρθηκε και προηγουμένως τα κύρια λάθη του συστήματος μετρούνται σε:

1) FRR (False Rejection Rate)
2) FAR (False Acceptance Rate)

Τα δυο αυτά ποσοστά εξαρτώνται από το κατώφλι αποδοχής t, το οποίο χρησιμοποιείται για να καθορίσει το επιθυμητό επίπεδο ασφάλειας. Για παράδειγμα ένα σύστημα με κατώφλι 99%, θα έχει περισσότερες λανθασμένες αποτυχίες ταιριάσματος και λιγότερα λανθασμένα ταιριάσματα από ένα σύστημα με κατώφλι 98%. Βέβαια η αποτελεσματικότητα κάθε συστήματος εξαρτάται από τις απαιτήσεις ασφαλείας. Αν για παράδειγμα μια εταιρία ενδιαφέρεται περισσότερο για την απαγόρευση της πρόσβασης θα χρησιμοποιήσει πολύ μεγάλο κατώφλι, αποδεχόμενη το ρίσκο της λανθασμένης αποτυχίας με αντίτιμο το μειωμένο ποσοστό πρόσβασης σε άτομα που δεν τη δικαιούνται. Η μαθηματική εξήγηση είναι η εξής: η συνάρτηση FRR(t) είναι αύξουσα, ενώ η συνάρτηση FAR(t) είναι φθίνουσα. Συνεπώς αν το κατώφλι αυξάνεται η πρόσβαση στους απατεώνες γίνεται πιο δύσκολη, όμως κάποιοι εξουσιοδοτημένοι χρήστες ίσως δυσκολευτούν να αποκτήσουν πρόσβαση στο σύστημα.



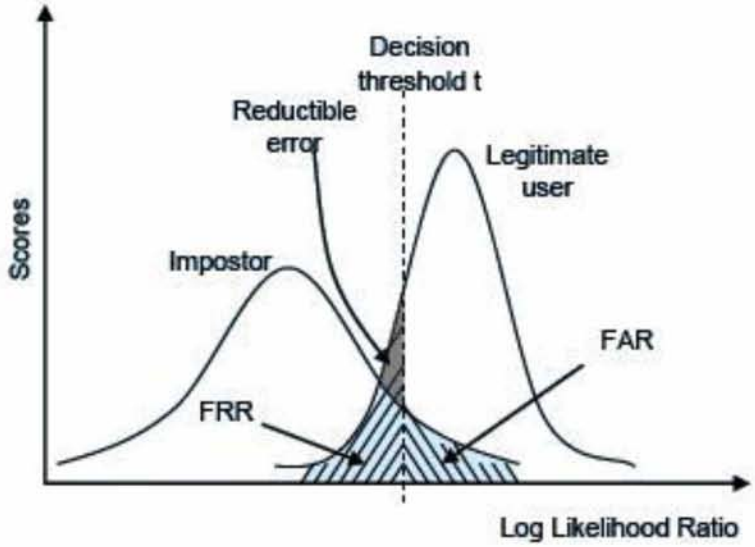
Γράφημα 1. Συναρτήσεις FRR(t) και FAR(t)

ERR (Equal Error Rate) : Δείχνει το λάθος του συστήματος όταν FRR=FAR

ZeroFRR: είναι το σημείο της FAR όταν FRR=0

ZeroFAR: είναι το σημείο της FRR όταν FAR=0

Το σημείο ERR, όπου FAR=FRR, υποδεικνύει την καλύτερη επιλογή για ένα βιομετρικό σύστημα μιας εφαρμογής πολιτών.



Γράφημα 2. Καμπύλες κατωφλίου απόφασης

Βιομετρική επαλήθευση (verification) ή θετική αυθεντικοποίηση (positive identification) (ταίριασμα 1 με 1)

Η επαλήθευση είναι ένα τεστ το οποίο διασφαλίζει ότι ένα άτομο Χ είναι όντως εκείνο το οποίο ισχυρίζεται πως είναι. Υπάρχουν δυο τύποι επαλήθευσης: με κεντρική αποθήκευση και με αποκεντρωτική αποθήκευση.

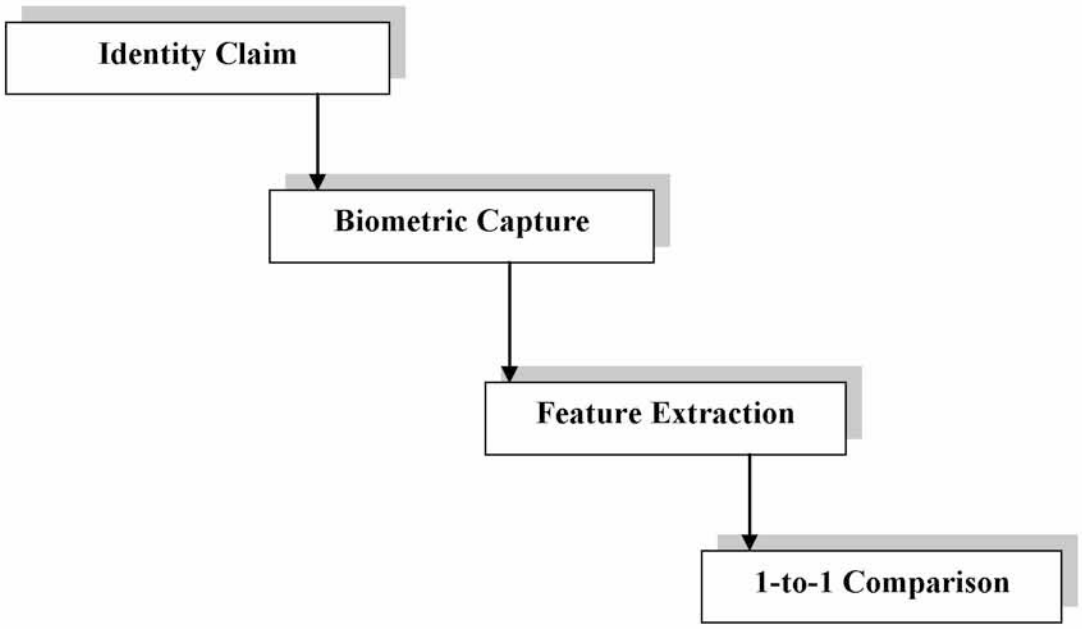
Επαλήθευση με κεντρική αποθήκευση

Προϋπόθεση είναι να υπάρχει μια κεντρική βάση δεδομένων, στην οποία βρίσκονται όλα τα βιομετρικά δεδομένα και οι συσχετιζόμενες ταυτότητες. Από εκεί γίνεται η ανάκτηση του βιομετρικού προτύπου της προς απόδειξη ταυτότητας. Το πρότυπο αυτό συγκρίνεται με το πρότυπο που παρέχεται από το άτομο Χ εκείνη τη στιγμή, έχοντας σαν αποτέλεσμα το ταίριασμα ή όχι. Δύο τύποι λαθών είναι δυνατόν να υπάρξουν κατά τη διαδικασία. Ένα λανθασμένο ταίριασμα, δηλαδή το άτομο Χ δεν είναι αυτό που ισχυρίζεται, αλλά το σύστημα λανθασμένα τον αποδέχεται, και μια λανθασμένη αποτυχία ταιριάσματος, δηλαδή το σύστημα λανθασμένα δεν αποδέχεται το άτομο Χ το οποίο είναι όντως αυτό το οποίο ισχυρίζεται πως είναι. Το ταίριασμα γίνεται τοπικά στη συσκευή αναγνώρισης ή οποία ανακαλεί προσωρινά το βιομετρικό πρότυπο της ταυτότητας που πρέπει να αποδειχθεί, από την κεντρική βάση δεδομένων.

Επαλήθευση με αποκεντρωμένη αποθήκευση

Αν το βιομετρικά δεδομένα είναι αποθηκευμένα σε μια μονάδα αποθήκευση, όπως μια smart card, η οποία βρίσκεται στην κατοχή του χρήστη, το άτομο Χ παρέχει ένα βιομετρικό πρότυπο τη στιγμή της διαδικασίας, το οποίο συγκρίνεται με το πρότυπο που βρίσκεται στο μέσο αποθήκευσης. Αυτή η διαδικασία γίνεται με δυο τρόπους. Η επαλήθευση γίνεται από το ίδιο το σύστημα, το οποίο ανακτά τα βιομετρικά δεδομένα του ατόμου Χ από τη μονάδα αποθήκευσης και συγκρίνοντάς τα με τα δεδομένα που παρέχονται εκείνη τη στιγμή. Ο άλλος τρόπος είναι να γίνεται η επαλήθευση μέσα στην ίδια τη μονάδα αποθήκευσης, αρκεί βέβαια να έχει την κατάλληλη υποδομή για να επιτελέσει μια τέτοια διαδικασία. Και εδώ υπάρχει ο κίνδυνος εμφάνισης των ίδιων λαθών, δηλαδή λανθασμένο ταίριασμα και λανθασμένη αποτυχία ταιριάσματος. Επιπρόσθετα υπάρχει ο κίνδυνος απώλειας, κλοπής ή αντιγραφής της μονάδας αποθήκευσης. Επίσης υπάρχει ο κίνδυνος τα

βιομετρικά δεδομένα της μονάδας αποθήκευσης να έχουν παραποιηθεί ή αλλοιωθεί, όπως για παράδειγμα μπορεί να συμβεί στα καινούργια βιομετρικά διαβατήρια.

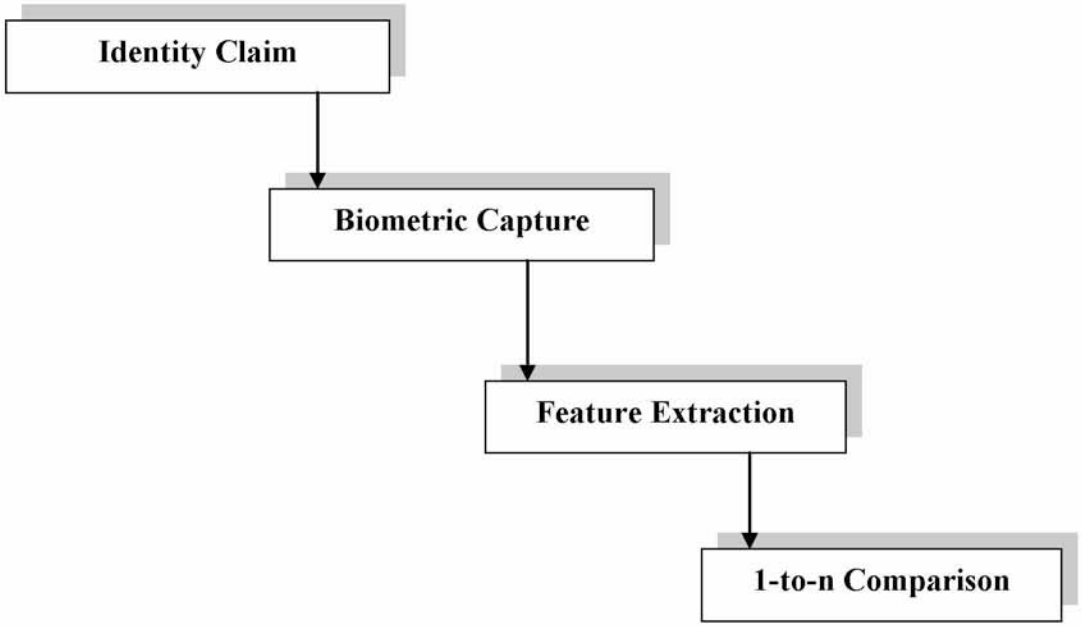


Εικόνα 9. Η διαδικασία της επαλήθευσης

Αυθεντικοποίηση (Identification) (ταίριασμα 1 με n)

Η αυθεντικοποίηση χρησιμοποιείται για να ανακαλύψει τη ταυτότητα ενός ατόμου όταν η ταυτότητα είναι άγνωστη, ο χρήστης δηλαδή δεν ισχυρίζεται / διεκδικεί καμία ταυτότητα. Αντίθετα με την επαλήθευση, στην αυθεντικοποίηση η ύπαρξη μιας κεντρικής μονάδας αποθήκευσης, η οποία περιέχει όλα τα άτομα που είναι γνωστά στο σύστημα, είναι απαραίτητη.

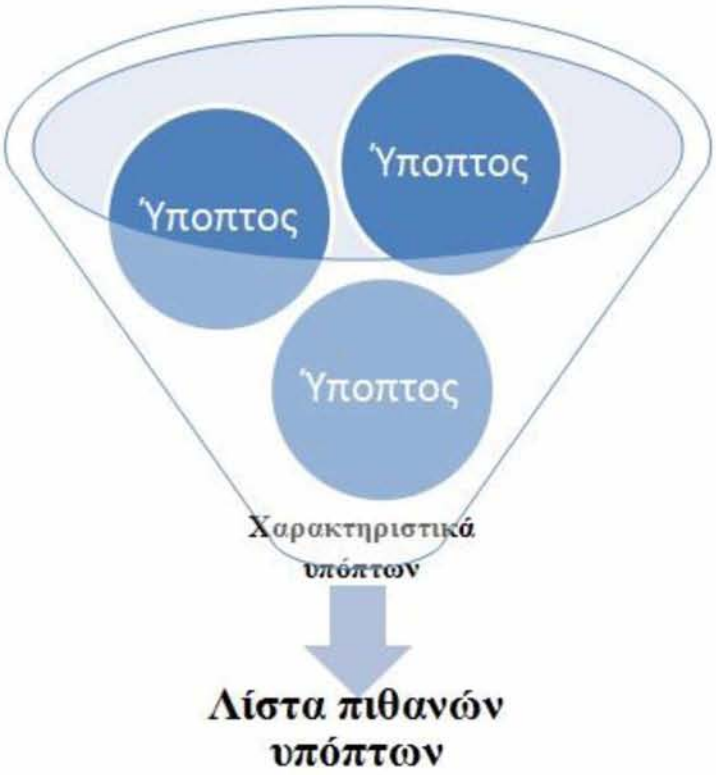
Όταν ο χρήστης Χ προσπαθήσει να αυθεντικοποιηθεί παρέχει ένα βιομετρικό πρότυπο το οποίο δημιουργείται εκείνη ακριβώς τη στιγμή, από μια διαδικασία αναγνώρισης, για παράδειγμα αναγνώριση δακτυλικών αποτυπωμάτων. Τα δεδομένα επεξεργάζονται και το προκύπτον βιομετρικό πρότυπο συγκρίνεται με όλα τα πρότυπα που βρίσκονται αποθηκευμένα στη βάση για να γίνει το ταίριασμα. Το σύστημα στη συνέχεια επιστρέφει είτε το ταίριασμα είτε ότι δεν υπάρχει ταίριασμα στον πληθυσμό της βάσης. Και σε αυτή τη διαδικασία υπάρχει πιθανότητα εμφάνισης των δυο λαθών που αναφέρθηκαν πιο πάνω, λανθασμένου ταιριάσματος και λανθασμένης αποτυχίας ταιριάσματος



Εικόνα 10. Η διαδικασία της αυθεντικοποίησης

Διαλογή (screening)

Μια ακόμη διαδικασία που έχει να κάνει με τα βιομετρικά συστήματα είναι η διαλογή (screening). Η διαλογή χρησιμοποιεί μια κεντρική βάση δεδομένων ή μια λίστα επίβλεψης (watch list). Μια τέτοια λίστα μπορεί να περιέχει βιομετρικά δεδομένα για ένα ζητούμενο άτομο ή μπορεί να περιέχει πληροφορίες για την ταυτότητα, με βάση την υπάρχουσα γνώση για το ζητούμενο άτομο. Με λίγα λόγια οι πληροφορίες αυτές είναι τα χαρακτηριστικά εκείνα που πρέπει να έχει κάποιος για να ταιριάζει στο προφίλ του προτύπου.



Εικόνα 11. Η διαδικασία της διαλογής

Ο διαχωρισμός αυτός ανάμεσα στην επαλήθευση, στην αυθεντικοποίηση και στη διαλογή βοηθά στην θεωρητική ανάλυση, στην πράξη όμως είναι δυνατόν αυτές οι δυο διαδικασίες να συνδυαστούν. Για παράδειγμα στην επιβολή του νόμου, η βιομετρία χρησιμοποιείται για να διαπιστώσει την παρουσία ενός υπόπτου στον τόπο του εγκλήματος, για να αναγνωρίσει ποιος ανάμεσα σε πολλούς υπόπτους βρισκόταν στον τόπο του εγκλήματος και για να δημιουργήσει το προφίλ ενός υπόπτου, ο οποίος ήταν παρών στον τόπο του εγκλήματος. Χρησιμοποιείται δηλαδή και για επαλήθευση και για αυθεντικοποίηση και για διαλογή.

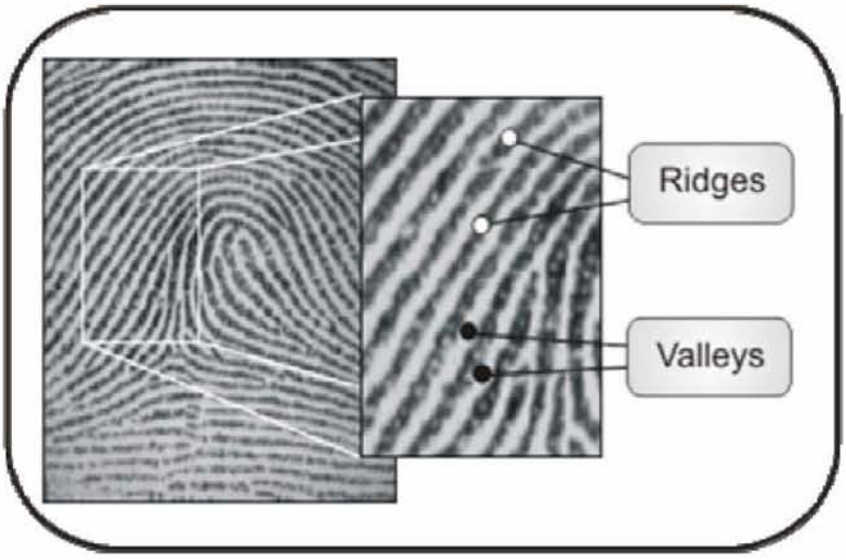
ΚΕΦΑΛΑΙΟ 2: ΚΥΡΙΕΣ ΒΙΟΜΕΤΡΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

Αναγνώριση δακτυλικού αποτυπώματος

Το ανθρώπινο δακτυλικό αποτύπωμα μπορεί να χρησιμοποιηθεί ως βιομετρικό χαρακτηριστικό μιας και το έχει κάθε άνθρωπος (καθολικότητα), είναι εμφανές διαχωρίσιμο μεταξύ δύο ατόμων (μοναδικότητα), είναι μόνιμο και αμετάβλητο κατά τη διάρκεια της ζωής του ατόμου (μονιμότητα) και μπορεί να μετρηθεί ποσοτικά (ικανότητα συλλογής).

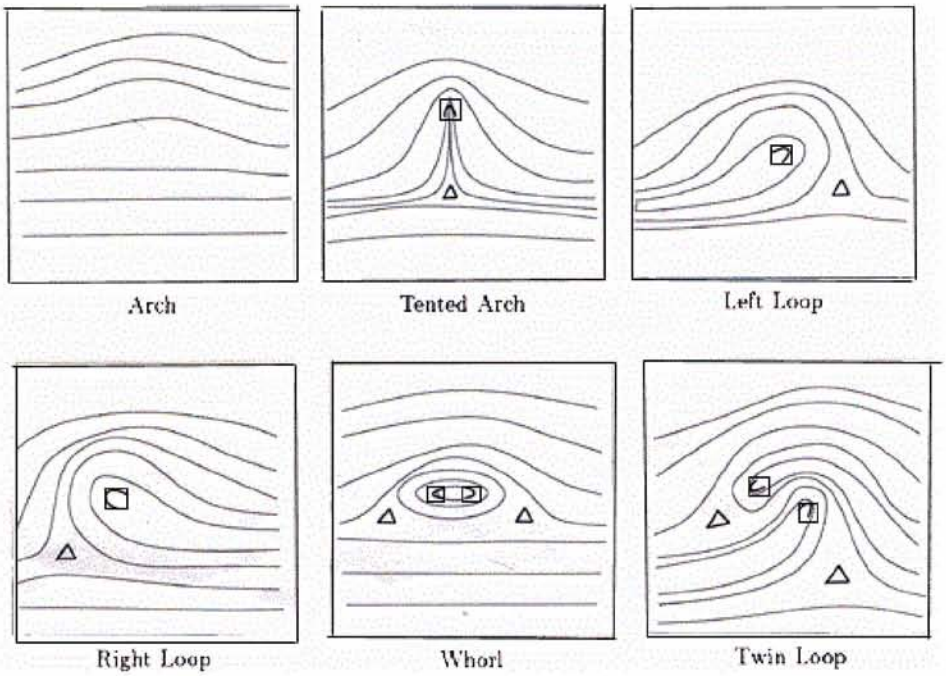
Το 19^{ο} αιώνα έγινε αποδεκτή, από την επιστημονική κοινότητα, η πρόταση ότι δεν υπάρχουν δυο άνθρωποι με ίδια δακτυλικά αποτυπώματα και ότι τα δακτυλικά αποτυπώματα δεν αλλάζουν σημαντικά κατά τη διάρκεια της ζωής ενός ατόμου. Αυτό ακριβώς αποτέλεσε την απαρχή της χρησιμοποίησης των δακτυλικών αποτυπωμάτων στην επιβολή του νόμου για την αναγνώριση εγκληματιών.

Τα χαρακτηριστικά των δακτυλικών αποτυπωμάτων καθορίζουν την μοναδικότητα και με βάση την θέση τους, το σχήμα τους και το μέγεθός τους γίνεται η αναγνώριση του ατόμου. Τα βασικότερα χαρακτηριστικά είναι οι διαδοχικές κοιλάδες (valleys) και παρυφές (ridges) της επιδερμίδας που βρίσκεται στο δακτυλικό αποτύπωμα. Συνήθως σε μια εικόνα δακτυλικού αποτυπώματος οι κοιλάδες είναι άσπρες και οι παρυφές μαύρες. Οι παρυφές έχουν πάχος συνήθως 100-300μm και οι κοιλάδες 200μm.



Εικόνα 12. Παρυφές και κοιλάδες δακτύλου

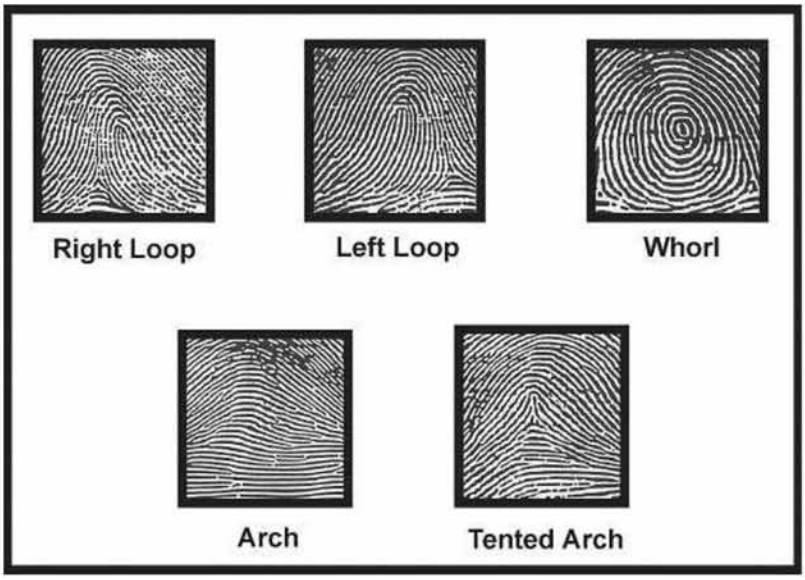
Συνήθως οι παρυφές και οι κοιλάδες βρίσκονται παράλληλα η μια στην άλλη μέχρι μια παρυφή να διακλαδωθεί σε δύο παρυφές ή να τερματίσει απότομα. Όταν αναλύουμε το δακτυλικό αποτύπωμα, μπορούμε να παρατηρήσουμε μία ή δύο περιοχές στις οποίες οι παρυφές και οι κοιλάδες έχουν συγκεκριμένα σχήματα. Αυτές οι περιοχές ονομάζονται ιδιαίτερες (singular regions) και διαχωρίζονται στις κατηγορίες: σημεία δέλτα (delta points) και σημεία πυρήνα (core points) και χαρακτηρίζονται από μεγάλη καμπυλότητα των παρυφών και των κοιλάδων και απότομων τερματισμών αυτών. Σημεία δέλτα είναι εκείνα τα σημεία στα οποία διασταυρώνονται παρυφές και κοιλάδες με τρεις διαφορετικές διευθύνσεις όπου κάθε διεύθυνση απέχει 120^{o} από τις άλλες δύο όπως παρουσιάζεται στο παρακάτω σχήμα με τρίγωνο. Τα σημεία πυρήνα απεικονίζονται με ένα τετράγωνο.



Εικόνα 13. Ιδιαίτερες περιοχές

Η διαφοροποίηση της καμπυλότητας των παρυφών και των κοιλάδων διαμορφώνει τις παρακάτω κατηγορίες:

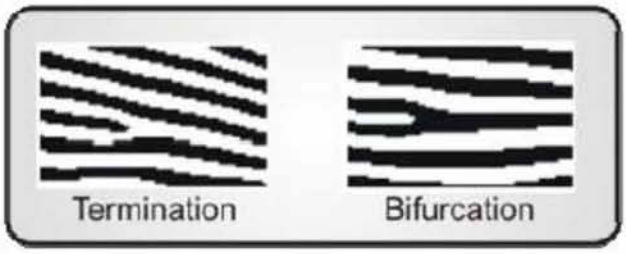
- Τόξο (Arch)
- Τεντωμένο Τόξο (Tented Arch)
- Αριστερός Βρόγχος (Left Loop)
- Δεξιός Βρόγχος (Right Loop)
- Δακτύλιος (Whorl)
- Διπλός Βρόγχος (Twin Loop)



Εικόνα 14. Ιδιαίτερες περιοχές

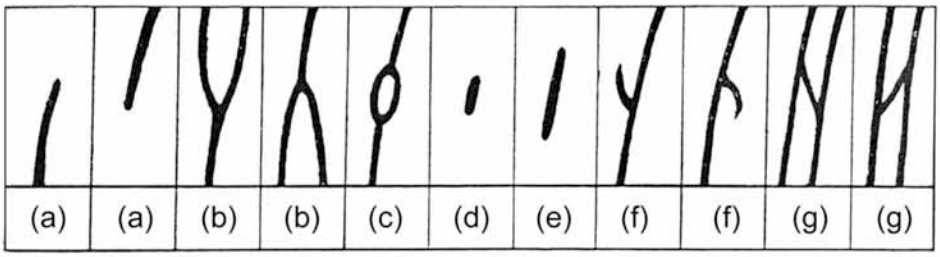
Οι ιδιαίτερες περιοχές χρησιμοποιούνται για την ταξινόμηση των δακτυλικών αποτυπωμάτων σε κατηγορίες με σκοπό την ταχύτερη, ευκολότερη και πιο αξιόπιστη αναζήτηση από μεγάλες βάσεις δεδομένων αποτυπωμάτων.

Οι ιδιαίτερες περιοχές (singular regions) μπορεί να χρησιμοποιούνται κυρίως για την ταξινόμηση των δακτυλικών αποτυπωμάτων σε κατηγορίες αλλά τα κύρια χαρακτηριστικά αναγνώρισης είναι η διακλάδωση των παρυφών και των κοιλάδων ή ο απότομος τερματισμός τους. Οι διακλαδώσεις (bifurcations) και οι τερματισμοί (terminations) των παρυφών ή των κοιλάδων αποτελούν τις μικρολεπτομέρειες (minutiae) ενός δακτυλικού αποτυπώματος και είναι τα κύρια χαρακτηριστικά αναγνώρισης του ατόμου από το σύστημα.



Εικόνα 15. Διακλάδωση και τερματισμός

Τα είδη των μικρολεπτομερειών που υπάρχουν παρουσιάζονται στην παρακάτω εικόνα, αν και τα συστήματα αναγνώρισης χρησιμοποιούν μόνο τις δύο πρώτες, γιατί όλες οι υπόλοιπες προκύπτουν από διακλαδώσεις και τερματισμούς:



Εικόνα 16. Τερματισμός (Termination), b) Διακλάδωση (Bifurcation), c) Λίμνη (Lake), d) Νησί (Island), e) Ανεξάρτητη Κορυφογραμμή (Independent Ridge), f) Σπιρούνι (Spur), g) Crossover

Τα δακτυλικά αποτυπώματα είναι πλήρη σχηματισμένα στον έβδομο μήνα ζωής του εμβρύου και δεν αλλάζουν κατά την διάρκεια ζωής του ατόμου εκτός της περίπτωσης που συμβεί κάποιο σοβαρό ατύχημα όπως βαθύ κόψιμο, έγκαυμα, ακρωτηριασμός . Εάν τα εγκαύματα ή τα κοψίματα είναι στην επιφάνεια του δέρματος ,δεν επηρεάζεται η δομή των παρυφών και των κοιλάδων γιατί η δομή αυτή θα αναπαραχθεί ξανά στο καινούργιο δέρμα που μεγαλώνει. Υπάρχουν τόσες πολλές μεταβολές κατά τον σχηματισμό του δακτυλικού αποτυπώματος, οι οποίες καθιστούν απίθανη την ταύτιση δύο δακτυλικών αποτυπωμάτων από δύο άτομα. Ακόμα και τα δακτυλικά αποτυπώματα των ομόζυγων διδύμων διαφέρουν παρόλο που σχηματίζονται από το ίδιο γονίδιο.

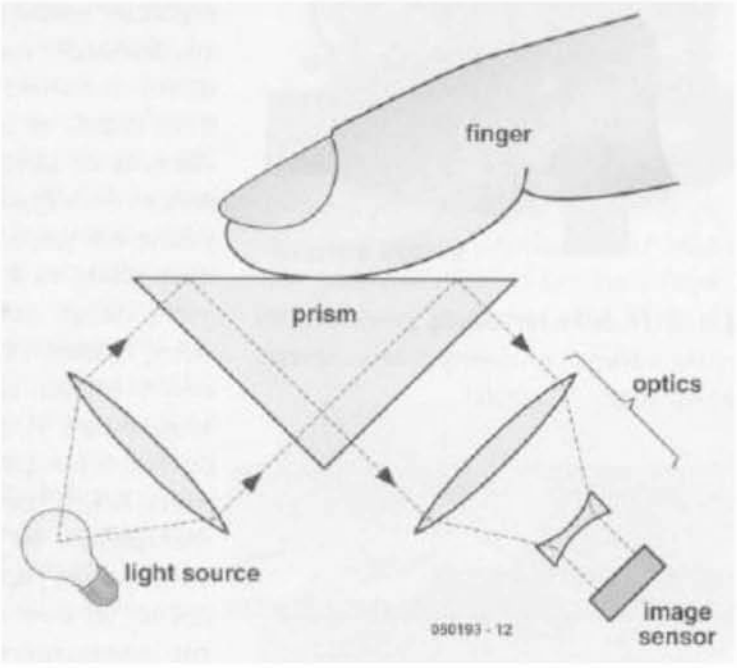
Οι απαιτήσεις ενός αισθητήρα αναγνώρισης δακτυλικού αποτυπώματος είναι οι εξής:

- Οι τιμές FAR (False Acceptance Rate) και FRR (False Rejection Rate) θα πρέπει να είναι οι ελάχιστες δυνατές.
- Το φυσικό μέγεθος θα πρέπει να είναι όσο το δυνατόν μικρότερο, για να είναι δυνατή η χρήση σε φορητές συσκευές.
- Ελάχιστη κατανάλωση ρεύματος.
- Αξιοπιστία και αντοχή.
- Δυνατότητα οικονομικής παραγωγής σε μαζική κλίμακα.

Οι αισθητήρες που βασίζονται σε ολοκληρωμένα, καταφέρνουν να ικανοποιήσουν τις περισσότερες από τις παραπάνω απαιτήσεις. Στο συγκεκριμένο τομέα υπάρχουν τόσες πολλές εξελίξεις που πραγματικά είναι πολύ δύσκολο να τις καλύψει όλες. Σε γενικές γραμμές, οι αισθητήρες είναι δυνατόν να ταξινομηθούν με βάση ορισμένες διαφορετικές αρχές λειτουργίας.

Η σημασία του αισθητήρα στο σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων είναι μεγαλύτερη από όλα τα άλλα μέρη του συστήματος. Είναι σημαντικό λοιπόν η ποιότητα της εικόνας του δακτυλικού αποτυπώματος που θα αποκτηθεί από τον αισθητήρα να είναι μεγάλη. Εάν η ποιότητα δεν είναι ικανοποιητική, όσο τέλειος και αποτελεσματικός είναι ο αλγόριθμος επεξεργασίας και αναγνώρισης ολόκληρο το σύστημα θα είναι αναξιόπιστο. Παρακάτω αναφέρονται κάποιες δημοφιλής τεχνολογίες αισθητήρων δακτυλικών αποτυπωμάτων.

Οπτικοί αισθητήρες ανάκλασης: Πρόκειται για την παλαιότερη τεχνική αναγνώρισης δακτυλικών αποτυπωμάτων. Το δάκτυλο τοποθετείται επάνω σε ένα γυαλί ή πρίσμα και φωτίζεται από ένα LED. Στο σημείο όπου οι κορυφές του δακτύλου ακουμπούν την επιφάνεια του γυαλιού το φώς απορροφάται, ενώ μεταξύ αυτών, στις κοιλάδες, έχουμε πλήρη ανάκλαση. Οι φωτεινές και σκοτεινές περιοχές που προκύπτουν, καταγράφονται από έναν οπτικό αισθητήρα (CCD ή CMOS).

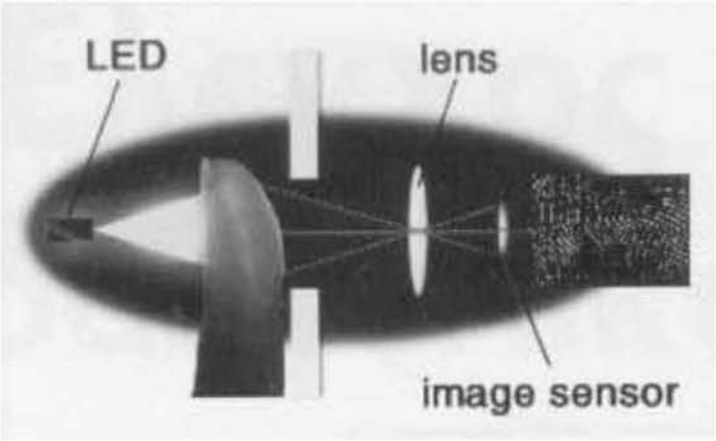


Εικόνα 17. Οπτική διάταξη με καταγραφή της εικόνας.

Στην πράξη βέβαια η συγκεκριμένη τεχνική παρουσιάζει αρκετά προβλήματα. Οι εικόνες που προκύπτουν από στεγνά ή βρεγμένα δάκτυλα διαφέρουν σημαντικά, ενώ είναι και ευαίσθητο στη σκόνη που μπορεί να επικαθίσει στην επιφάνεια. Η μονάδα παρουσιάζει μεγάλο μέγεθος και είναι ακριβή. Εάν το δέρμα είναι φθαρμένο ή έχει

εκδορές, το αποτύπωμα συχνά δεν αναγνωρίζεται. Στην περίπτωση που η εικόνα αναφοράς έχει ληφθεί με μικρότερη πίεση στο δάκτυλο, είναι πιθανό το FAR να είναι υψηλό.

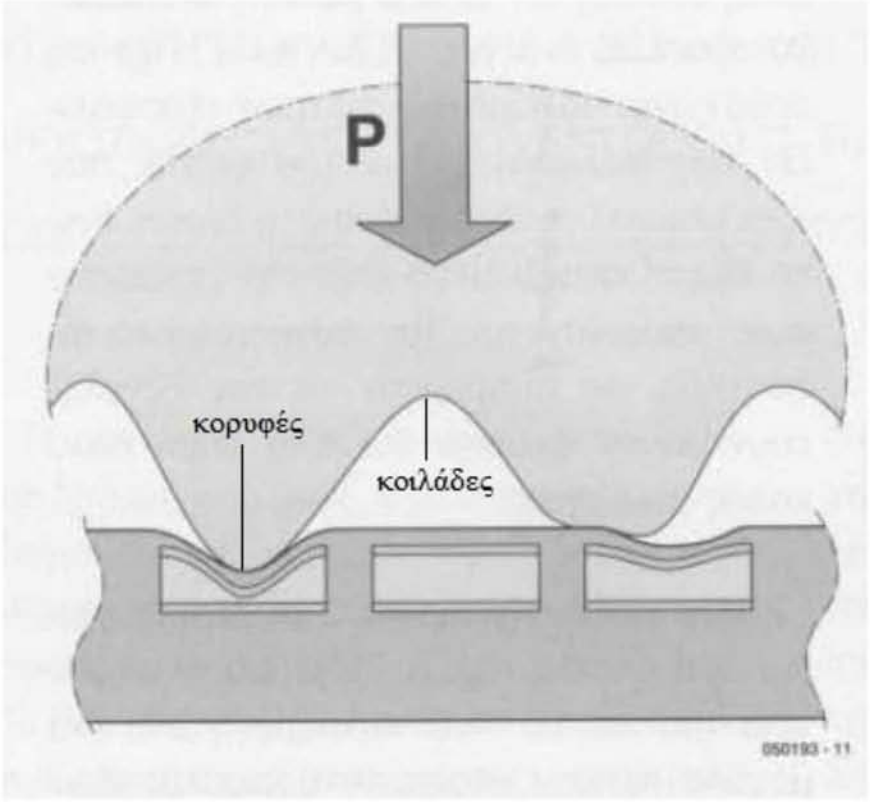
Οπτικοί αισθητήρες μετάδοσης: Η συγκεκριμένη τεχνική λειτουργεί χωρίς να απαιτείται άμεση επαφή μεταξύ του δακτύλου και της επιφάνειας του αισθητήρα. Σε μια διάταξη που έχει κυκλοφορήσει η Mitsubishi (Mitsubishi MyPass LP-1002), μια δέσμη φωτός διέρχεται από το δάκτυλο από την πάνω πλευρά, εκεί που βρίσκεται το νύχι και στη συνέχεια μια κάμερα παίρνει φωτογραφία του δακτυλικού αποτυπώματος. Η εταιρεία Lumidigm (http://www.lumidigm.com/) χρησιμοποιεί μια πιο σύνθετη προσέγγιση. Οι μετρήσεις γίνονται με χρήση φωτισμού διαφορετικών μηκών κύματος. Ο αισθητήρας "βλέπει" μέσα από την επιφάνεια του δέρματος, τον υποδόριο ιστό, και παράγει μια πολυ-φασματική εικόνα. Η χρήση διαφορετικών μηκών κύματος για τη δημιουργία εικόνων, αναδεικνύει διαφορετικές υποδόριες δομές. Αυτό το χαρακτηριστικό μας προσφέρει μια επιπλέον δικλείδα ασφαλείας, ότι το δάκτυλο που ερευνάται είναι αληθινό. Στην τεχνική αυτή η υγρασία δεν έχει καμία επίδραση.



Εικόνα 18. Διάταξη από Mitsubishi

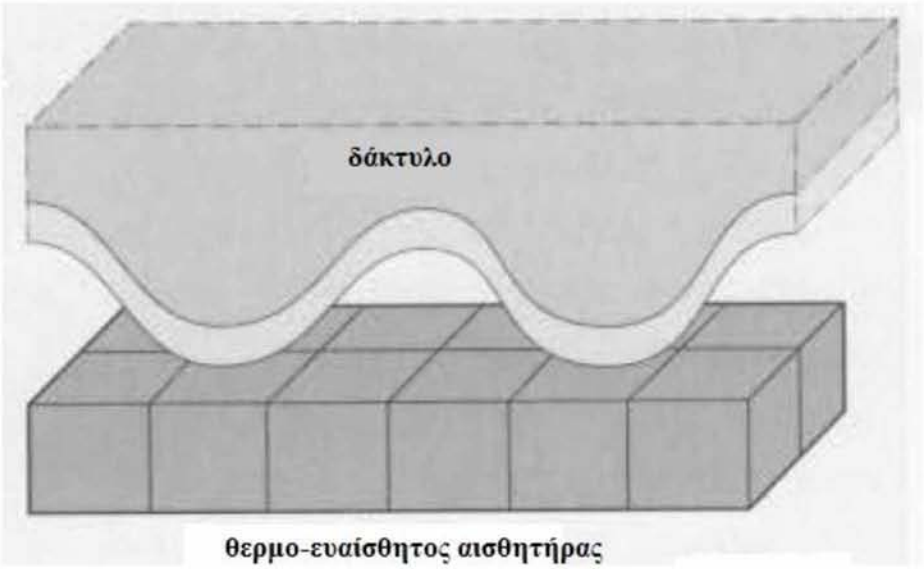
Μηχανικοί αισθητήρες: Ο συγκεκριμένος τύπος αισθητήρα αποτελεί την πλέον γενική μορφή συσκευής MEMS (Micro Electro-Mechanical System, Μικρό Ηλεκτρο-Μηχανικό Σύστημα https://www.memsnet.org/mems/what-is.html). Σε μια διάταξη, η οποία έχει αναπτυχθεί στο από το Γαλλικό Ινστιτούτο Ερευνών LETI (http://www.leti.fr/en), τοποθετούνται δεκάδες χιλιάδες μικροσκοπικοί μορφοτροπείς

πίεσης (αισθητήρια στοιχεία), διατεταγμένοι στην επιφάνεια του αισθητήρα. Μια εναλλακτική σχεδίαση χρησιμοποιεί μικρο-διακόπτες οι οποίοι μόλις πατηθούν από μια κορυφή κλείνουν επαφή, ενώ όταν εφάπτεται κοιλάδα παραμένουν ανοικτοί. Με τον τρόπο αυτό έχουμε ένα μόλις ψηφίο πληροφορίας για κάθε αισθητήριο στοιχείο, αντί να έχουμε κλίμακα του γκρι.



Εικόνα 19.Διάταξη με μικρο-αισθητήρες πίεσης.

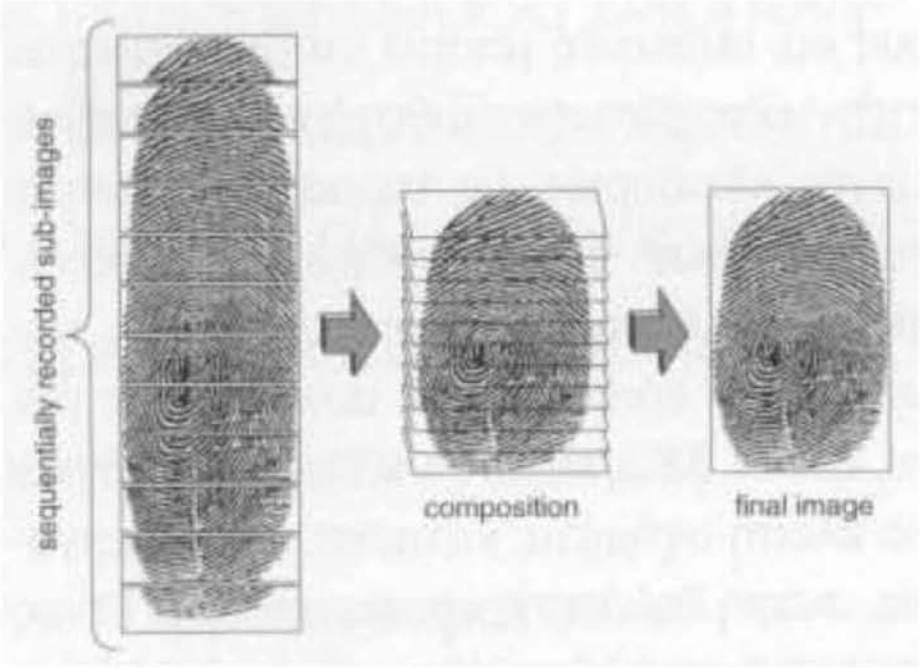
Θερμικοί αισθητήρες: Ο αισθητήρας ανιχνεύει τη θερμότητα του δέρματος, η οποία είναι μεγαλύτερη στις κορυφές και μικρότερη στις κοιλάδες. Πρωτοπόρος στη συγκεκριμένη τεχνολογία είναι η Atmel (http://www.atmel.com/) , η οποία έχει αναπτύξει μια μονάδα πυριτίου με ένα πίνακα αισθητηρίων στοιχείων, το οποίο καλείται FingerChip, όπου το κάθε στοιχείο καλύπτεται από στρώμα πυροηλεκτρικού υλικού στο οποίο η μεταβολή στη θερμοκρασία οδηγεί σε μεταβολή της επιφανειακής κατανομής φορτίου. Το κάθε στοιχείο συνοδεύεται από ένα ενισχυτή ο οποίος μεταφέρει το σήμα στο κύκλωμα αναγνώρισης. Εκεί δημιουργείται μια εικόνα σε τόνους του γκρι, η οποία παρουσιάζει ικανοποιητική ποιότητα ακόμη και με βρεγμένα, βρώμικα ή φθαρμένα δάκτυλα.



Εικόνα 20. Η αρχή λειτουργίας ενός θερμικού αισθητήρα

Εικόνα 21. Ο αισθητήρας της Atmel, FingerChip.

Αισθητήρες δυναμικής εξόδου: Αντί το δάκτυλο να τοποθετείται απλά πάνω στον αισθητήρα, απαιτείται ένα αργό σύρσιμο του δακτύλου επάνω σε αυτόν. Ο αισθητήρας διαθέτει μια ευαίσθητη ζώνη αναγνώρισης η οποία είναι στενή και παράγει μια ολοκληρωμένη ακολουθία εικόνων, τις οποίες ο επεξεργαστής είναι σε θέση να ολοκληρώσει σε μια πλήρη εικόνα. Με τον τρόπο αυτό αυξάνεται σημαντικά η αξιοπιστία, ενώ οποιοδήποτε ίχνος βρωμιάς θα απομακρυνθεί. Αισθητήρες αυτής της μορφής κατασκευάζουν αρκετές εταιρείες, μεταξύ των οποίων και η UPEK.



Εικόνα 22. Ακολουθιακή καταγραφή εικόνων και σύνθεσή τους σε μια ολοκληρωμένη εικόνα

Εικόνα 23. Eikon-to-go. Αισθητήρας της UPEK

Εξαγωγή χαρακτηριστικών

Αρχικά η εικόνα που δημιουργείται είναι σε μορφή ακατέργαστη, με την οποία δεν μπορούμε να κάνουμε και πολλά, δεδομένου ότι απαιτούνται μεγάλα ποσά μνήμης και η οποιαδήποτε απόπειρα σύγκρισης με άλλες εικόνες θα απαιτούσε μεγάλη επεξεργαστική ισχύ. Αντί αυτού, εξάγουμε από την εικόνα κάποια χαρακτηριστικά, τις μικρολεπτομέρειες που έχουν ήδη αναφερθεί. Η εξαγωγή του προσανατολισμού και της θέσης των χαρακτηριστικών αυτών είναι αρκετή για να προκύψει ένας σαφής χαρακτηρισμός. Από 20-100 μικρολεπτομέρειες είναι υπεραρκετές για να έχουμε μια αξιόπιστη κρίση. Τα δεδομένα που εξάγονται απαιτούν πολύ μικρότερο όγκο μνήμης για να αποθηκευτούν. Αυτά τα δεδομένα στη συνέχεια επεξεργάζεται ο υπολογιστής, οπότε δίνεται η δυνατότητα για πολύ μεγάλο αριθμό συγκρίσεων σε σχετικά σύντομο χρονικό διάστημα.

Μπορούμε να “ξεγελάσουμε” ένα σύστημα βιομετρικής αναγνώρισης;

Τον πρώτο καιρό εφαρμογής της συγκεκριμένης τεχνολογίας, η εξαπάτηση του ανιχνευτή ήτα σχετικά εύκολη υπόθεση. Η αρχική ιδέα ήταν να αναδημιουργούνται τα ίχνη λίπους που παραμένουν στον αισθητήρα από τον προηγούμενο έλεγχο (δάκτυλο άλλου ατόμου). Εκπνέοντας λοιπόν στην επιφάνεια του αισθητήρα, μικρά σταγονίδια υγρασίας η εικόνα γίνεται καθαρότερη. Με τον τρόπο αυτό οι αισθητήρες που χρησιμοποιούσαν οπτική τεχνολογία εξαπατούνταν. Η δυναμική τεχνική αναπτύχθηκε με σκοπό να ξεπεραστεί το συγκεκριμένο πρόβλημα, αφού το δάκτυλο δεν τοποθετείται πλέον πάνω στον αισθητήρα, αλλά σύρεται αργά πάνω σε αυτόν. Με τον τρόπο αυτό τα παλιά ίχνη λίπους εξαφανίζονται.

Μια δεύτερη τεχνική εξαπάτησης είναι να εφαρμόζεται στον αισθητήρα ένα αντίγραφο του δακτυλικού αποτυπώματος. Όπως είναι γνωστό, οι άνθρωποι αφήνουν δακτυλικά αποτυπώματα παντού. Η λήψη αντιγράφων των αποτυπωμάτων αυτών είναι μια τεχνική που χρησιμοποιείται κατά κόρον από την υπηρεσία σήμανσης της αστυνομίας. Η λεπτή σκόνη γραφίτη κολλάει στα ίχνη λίπους που αφήνει το δάκτυλο και στη συνέχεια το σχέδιο του γραφίτη μεταφέρεται σε κολλητική ταινία. Η τεχνική αυτή μπορεί να εξαπατήσει ακόμη και τους δυναμικούς αισθητήρες. Για να αποφευχθεί αυτό, δημιουργήθηκαν οι θερμικοί και οι μηχανικοί αισθητήρες.

Διαδικασία

Η διαδικασία της εγγραφής των δακτυλικών αποτυπωμάτων ενός ατόμου στη βάση δεδομένων στο σύστημα αναγνώρισης γίνεται και στα δυο είδη αναγνώρισης. Κατά την διαδικασία της εγγραφής, το αποτύπωμα του ατόμου συλλαμβάνεται από κάποιον αισθητήρα και μετατρέπεται σε ψηφιακό σήμα. Ακολούθως πραγματοποιείται ένας έλεγχος ποιότητας με σκοπό να επιβεβαιωθεί ότι το συγκεκριμένο δείγμα μπορεί να επεξεργαστεί επιτυχώς στα επόμενα στάδια επεξεργασίας. Στο επόμενο στάδιο ακολουθεί μια προ-επεξεργασία με σκοπό την βελτίωση κάποιων χαρακτηριστικών του δείγματος, ώστε να επιτευχθεί η καλύτερη εξαγωγή των μικρολεπτομερειών, οι οποίες στο στάδιο της σύγκρισης θα χρησιμοποιηθούν για την αναζήτηση από την βάση δεδομένων. Η εξαγωγή κάποιων συγκεκριμένων χαρακτηριστικών γίνεται τόσο για να μειωθεί ο χρόνος αναζήτησης από την βάση και η επεξεργαστική ισχύ όσο και να αυξηθεί η αξιοπιστία της αναζήτησης. Τα πρότυπα που παράγονται από το στάδιο εξαγωγής θα χρησιμοποιηθούν για την αναγνώριση, για αυτό αποθηκεύονται σε μια βάση βιομετρικών δεδομένων μαζί με το όνομα του ατόμου που αντιστοιχούν αυτά τα αποτυπώματα.

Εικόνα 24. Στάδιο εξαγωγής προτύπου

Στην περίπτωση του συστήματος αυθεντικοποίησης ο χρήστης εισάγει το όνομά του και ακολούθως εισάγει το δακτυλικό του αποτύπωμα. Ο αισθητήρας το μετατρέπει σε ψηφιακό σήμα και εφόσον προχωρήσει στο επίπεδο ταιριάσματος, γίνεται σύγκριση μόνο με τα αποτυπώματα του γνήσιου χρήστη που είναι αποθηκευμένα στη βάση δεδομένων του συστήματος.

Εικόνα 24. Στάδιο Αυθεντικοποίησης Χρήστη

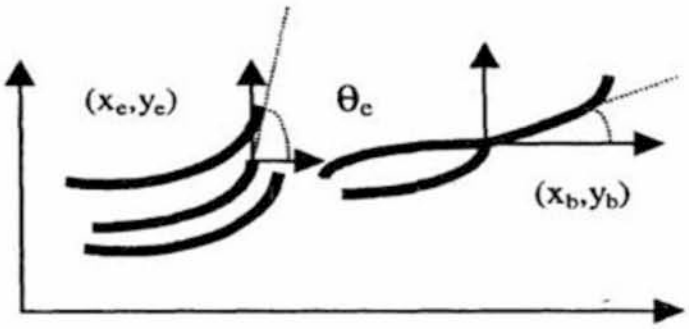
Στην περίπτωση της αναγνώρισης/ταυτοποίησης δεν εισάγεται όνομα και το σύστημα συγκρίνει τα χαρακτηριστικά που λήφθηκαν από το δακτυλικό αποτύπωμα του χρήστη με όλα τα χαρακτηριστικά όλων των χρηστών που είναι αποθηκευμένα στην βάση του συστήματος. Η έξοδος ενός συστήματος ταυτοποίησης είναι η ταυτότητα του χρήστη με το αποτύπωμα που τοποθετήθηκε στην είσοδο του συστήματος ή ένα μήνυμα που δηλώνει ότι ο χρήστης δεν βρέθηκε στην βάση δεδομένων (user not identified). Όταν οι βάσης βιομετρικών δεδομένων είναι πολύ μεγάλες χρησιμοποιούνται και τεχνικές ταξινόμησης των βιομετρικών χαρακτηριστικών σε κατηγορίες προκειμένου να ελαχιστοποιηθεί ο χρόνος αναζήτησης και η ανάγκη για μεγάλη υπολογιστική ισχύ του συστήματος αναγνώρισης.

Εικόνα 25. Στάδιο Ταυτοποίησης Χρήστη

Αλγόριθμος αναγνώρισης αποτυπωμάτων με εντοπισμό μικρολεπτομερειών

Σε ένα δακτυλικό αποτύπωμα, όπως αναφέρθηκε, μπορούν να παρατηρηθούν τοπικές αυλακώδεις ασυνέχειες γνωστές και ως μικρολεπτομέρειες. Υπάρχουν δύο χαρακτηριστικοί τύποι μικρολεπτομερειών, οι διακλαδώσεις και τα τελειώματα.

Ένας ενδιαφέρων αλγόριθμος προς την κατεύθυνση της αναγνώρισης με εντοπισμό των μικρολεπτομερειών, προτάθηκε από την Virginia Espinosa-Duro. (Virginia Espinosa-Duro "Minutiae Detection Algorithm for Fingerprint Recognition" IEEE AESS Systems Magazine, March 2002.) Για τη αξιόπιστη εφαρμογή της συγκεκριμένης τεχνικής θα πρέπει να εξαχθούν περίπου 40-100 μικρολεπτομέρειες. Θα πρέπει δηλαδή, να εντοπίσουμε τις κορυφογραμμές τερματισμού και διακλάδωσης. Τα δυο αυτά είδη μικρολεπτομέρειας περιγράφονται από τη θέση τους (συντεταγμένες x, y) και από τον προσανατολισμό τους (γωνία θ).



Εικόνα 26. Περιγραφή μικρολεπτομερειών από τη θέση και τον προσανατολισμό

Ο εντοπισμός κάθε μικρολεπτομέρειας σε αυτόν τον αλγόριθμο χρησιμοποιεί ένα απλό πρότυπο αναγνώρισης. Αν ένα εικονοστοιχείο βρίσκεται σε μια λεπτή κορυφογραμμή (με οκτώ γειτονικά εικονοστοιχεία), τότε λαμβάνει την τιμή *1*, διαφορετικά την τιμή *0*. Αν υποτεθεί ότι ένα **εικονοστοιχεία** πάνω σε μια λεπτή κορυφογραμμή δηλώνεται ως (x, y) και N_0 έως N_7 δηλώνονται τα γειτονικά του εικονοστοιχεία, τότε ισχύουν τα εξής:

- Τελείωμα : $\sum_{i=0}^{7} N_i = 1$
- Διακλάδωση : $\sum_{i=0}^{7} N_i > 2$

Η τελική δομή των κορυφογραμμών θα χρησιμοποιηθεί για την εξαγωγή του *Χάρτη μικρολεπτομερειών*, ο οποίος χαρακτηρίζει και το δακτυλικό αποτύπωμα. Αυτός ο χάρτης θα σχηματίσει ένα πρότυπο που θα περιλαμβάνει μια λίστα με μικρολεπτομέρειες και μια λίστα με τον αριθμό των κορυφογραμμών μεταξύ των ζευγαριών μικρολεπτομέρειας. Τα πειραματικά αποτελέσματα αυτής της μεθόδου έδειξαν ότι το σύστημα αυτό αναγνώρισε τις περισσότερες μικρολεπτομέρειες που

υπάρχουν στην αρχική εικόνα, αλλά ο αριθμός αυτός εξαρτάται σε μεγάλο βαθμό από το σύστημα λήψης της εικόνας.

Προβλήματα στην αναγνώριση δακτυλικών αποτυπωμάτων

Η διαδικασία αναγνώρισης δακτυλικών αποτυπωμάτων αποτελεί μια δύσκολη και απαιτητική διαδικασία. Δεν είναι τυχαίο το γεγονός ότι μέχρι σήμερα πολλά από τα υπάρχοντα συστήματα που χρησιμοποιούνται στην καθημερινή πρακτική παρουσιάζουν μειονεκτήματα. Υπάρχει σημαντική βιβλιογραφική καταγραφή διεθνώς όσον αφορά στην ανάπτυξη τεχνικών και αλγορίθμων για τη βελτίωση των σφαλμάτων αυτών και τη διασφάλιση της ποιότητας του αποτελέσματος που συλλέγεται. Τα κυριότερα προβλήματα είναι:

1. **Τρόπος τοποθέτησης του δακτύλου:** ο τρόπος με τον οποίο τοποθετείται το δάκτυλο πάνω στην επιφάνεια σάρωσης επηρεάζει σημαντικά τη διαδικασία. Ακόμη και αν οι λήψεις γίνουν διαδοχικά, οι εικόνες που προκύπτουν μπορεί να διαφέρουν κατά οριζόντια ή κατακόρυφη μετατόπιση καθώς και κατά γωνία. Αυτό επιβαρύνει τη διαδικασία ευθυγράμμισης του αποτυπώματος που απαιτείται πριν από τη σύγκριση. Πρόβλημα επίσης μπορεί να προκύψει από την πίεση που θα ασκήσει το άτομο στο δάκτυλό του, κατά την αποτύπωση. Αν δηλαδή σε μια λήψη το άτομο πιέσει περισσότερο το δάκτυλο σε μια από τις διαδοχικές λήψεις, το αποτύπωμα θα υποστεί μη γραμμική παραμόρφωση.
2. **Μεταβολές δακτυλικού αποτυπώματος:** Η παραμόρφωση του δακτυλικού αποτυπώματος μπορεί να οφείλονται σε αλλοιώσεις λόγω εγκαύματος, ακρωτηριασμού ή εξαιτίας κάποιας αμυχής. Αυτή η παραμόρφωση είναι λογικό να δυσχεράνει την διαδικασία ιδιαίτερα στην περίπτωση που γίνεται σύγκριση με εικόνα που είχε ληφθεί πριν από την αλλοίωση.
3. **Ύπαρξη θορύβου:** ως θόρυβος χαρακτηρίζεται οποιαδήποτε πληροφορία εμπεριέχεται στη συλλεγμένη εικόνα του δακτυλικού αποτυπώματος η οποία δε σχετίζεται με τα κύρια χαρακτηριστικά του. Μπορεί να εισάγεται στην εικόνα είτε κατά τη διάρκεια της συλλογής δεδομένων (ύπαρξη μικρών στοιχειών - σκουπιδιών) είτε από τον τρόπο ψηφιοποίησης και δημιουργίας της εικόνας από το σύστημα συλλογής.

Που μπορεί να συναντήσουμε βιομετρικά συστήματα αναγνώρισης δακτυλικού αποτυπώματος.

Μπορούμε να συναντήσουμε συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων σε κλειδαριές, σε φορητούς υπολογιστές, σε πληκτρολόγια και σε σημεία εισόδου κυρίως επιχειρήσεων, ακόμη και στον έλεγχο πρόσβασης στα σύνορα.

Εικόνα 27. Κλειδαριά με βιομετρικό αναγνώστη δακτυλικού αποτυπώματος

Εικόνα 28. Πρόσβαση σε χώρο με τη χρήση smart card και δακτυλικού αποτυπώματος

Εξαιτίας της σχετικά φτηνής τεχνολογίας που απαιτείται για ένα σαρωτή και της μικρής υπολογιστικής ισχύος που απαιτείται για την αναγνώριση ενός ατόμου, η βιομετρική τεχνολογία συναντάται και στα κινητά τηλέφωνα, ακόμη και σε αντικλεπτικά συστήματα αυτοκινήτων και μηχανών.

Εικόνα 29. Σύστημα εκκίνησης κινητήρα αυτοκινήτου με βιομετρικό αναγνώστη δακτυλικού αποτυπώματος

Εικόνα 30. Κινητό τηλέφωνο με ενσωματωμένο βιομετρικό αναγνώστη δακτυλικού αποτυπώματος

Υπάρχουν επίσης εφαρμογές που αντικαθιστούν το γνωστό "χτύπημα της κάρτας" των εργαζομένων και ονομάζονται Fingerprint attendance systems.

Εικόνα 31. Σύστημα παρακολούθησης παρουσίας

Integrated Automated Fingerprint Identification System (IAFIS)

Το σύστημα IAFIS είναι ένα εθνικό αυτόματο σύστημα αναγνώρισης δακτυλικού αποτυπώματος το οποίο διατηρείται από το FBI. Το σύστημα αυτό κατέχει τη μεγαλύτερη βιομετρική βάση δεδομένων στον κόσμο, περιέχοντας τα αποτυπώματα και το ιστορικό για πάνω από 55εκατομμύρια άτομα.

Τα δακτυλικά αποτυπώματα δίνονται εθελοντικά στο FBI από τοπικές ή ομοσπονδιακές αρχές επιβολής του νόμου. Τα δακτυλικά αποτυπώματα προέρχονται συνήθως από συλλήψεις εγκληματιών ή από άλλες πηγές όπως έλεγχο υπαλλήλων και μέσω του προγράμματος US-VISIT. Το FBI στη συνέχεια κατηγοριοποιεί τα αποτυπώματα και τα συνδέει με τυχόν εγκληματικό παρελθόν του ατόμου. Έτσι οι αρχές μπορούν να ζητήσουν μια έρευνα αποτυπωμάτων από το IAFIS για την αναγνώριση ενός υπόπτου σε εγκληματολογικές έρευνες.

Αναγνώριση προσώπου

Η κατασκευή συστημάτων που θα έχουν τη δυνατότητα να επιλύουν πολύπλοκα ή χρονοβόρα προβλήματα υπήρξε αντικείμενο έρευνας πολλών επιστημόνων. Στόχος είναι η διεύρυνση των ικανοτήτων των υπολογιστών και η ανάπτυξη κατάλληλων εφαρμογών που να αντιμετωπίζουν αυτά τα προβλήματα. Βασικός παράγοντας προκειμένου να γίνει αυτό είναι η δυνατότητα των υπολογιστών να αναγνωρίζουν το περιβάλλον μέσα στο οποίο λειτουργούν, δηλαδή να μπορούν να εκτιμήσουν την δεδομένη κατάσταση κάνοντας διάφορες μετρήσεις και στη συνέχεια να πάρουν την κατάλληλη απόφαση. Αμέσως λοιπόν φαίνεται η ανάγκη για την ανάπτυξη αλγορίθμων που καθιστούν ικανούς τους υπολογιστές να αναγνωρίσουν τα αντικείμενα που επεξεργάζονται, ή αλλιώς τα διάφορα πρότυπα. Στα πλαίσια της ανάπτυξης αλγορίθμων αναγνώρισης προτύπων εντάσσεται και η ανάπτυξη αλγορίθμων για την αναγνώριση προσώπων.

Η αναγνώριση προσώπων έχει γνωρίσει τα τελευταία χρόνια ιδιαίτερη ανάπτυξη, γεγονός που οφείλεται κυρίως στο μεγάλο εύρος των εφαρμογών που χρησιμοποιούν συστήματα αναγνώρισης προσώπων και την διαθεσιμότητα κατάλληλης τεχνολογίας μετά από πολλά χρόνια έρευνας. Επιπλέον, το πρόβλημα της αναγνώρισης εικόνων του ανθρώπινου προσώπου από τον υπολογιστή εξακολουθεί να προσελκύει ερευνητές που δραστηριοποιούνται στις περιοχές της επεξεργασίας εικόνας, της αναγνώρισης προτύπων, των νευρωνικών δικτύων, της υπολογιστικής όρασης, των γραφικών του υπολογιστή κ.α.

Παρά το γεγονός πως υπάρχουν πολύ αξιόπιστες μέθοδοι βιομετρικής πιστοποίησης της ταυτότητας, όπως για παράδειγμα η ανάλυση των αποτυπωμάτων και η σάρωση της ίριδας, αυτές οι μέθοδοι βασίζονται στη συνεργασία των χρηστών, ενώ αντίθετα ένα σύστημα εξακρίβωσης ταυτότητας που βασίζεται στην ανάλυση εικόνων του ανθρώπινου προσώπου είναι συχνά πολύ αποτελεσματικό χωρίς τη συμμετοχή του χρήστη. Οι εφαρμογές της αναγνώρισης προσώπων είναι πολυπληθείς: συστήματα ασφαλείας, έλεγχος πρόσβασης τόσο στα σύνορα όσο και σε εσωτερικούς χώρους, εγκληματολογία, αλληλεπίδραση ανθρώπου-υπολογιστή (αναγνώριση εκφράσεων), κ.α.

Η αυτόματη αναγνώριση προσώπου είναι μια σχετικά νέα έννοια. Τη δεκαετία του 1960, το πρώτο ημι-αυτόματο σύστημα αναγνώρισης προσώπου, απαιτούσε ο διαχειριστής να εντοπίσει χαρακτηριστικά (όπως μάτια, αυτιά, μύτη και στόμα) πάνω

στην φωτογραφία, πριν υπολογίσει αποστάσεις και ποσοστά προς ένα σημείο αναφοράς και τα οποία στη συνέχεια συγκρίνονταν με τα δεδομένα προτύπου.

Ένα πρόσωπο είναι μια τρισδιάστατη στερεή επιφάνεια, η οποία διαθέτει τμήματα που είναι μερικώς παραμορφώσιμα. Οι εικόνες του προσώπου που παράγονται εξαρτώνται από τον προσανατολισμό του, την οπτική γωνία, τις συνθήκες φωτισμού, τις εκφράσεις, την ηλικία, τα προϊόντα καλλωπισμού που χρησιμοποιούνται κ.α. Οι δύο κύριες προσεγγίσεις στην αναγνώριση προσώπων είναι αυτές που χρησιμοποιούν δισδιάστατες μεθόδους στηριγμένες στην εμφάνιση ή στα χαρακτηριστικά και αυτές που χρησιμοποιούν μεθόδους που στηρίζονται σε τρισδιάστατα μοντέλα. Η μεγάλη πλειοψηφία των μεθόδων που έχουν προταθεί ανήκει στην πρώτη κατηγορία.

Τα πρώτα πρωτότυπα για συστήματα αναγνώρισης προσώπου αναπτύχθηκαν στις αρχές τις δεκαετίας του 1990. Το 1993, το υπουργείο άμυνας των ΗΠΑ, έστησε το πρόγραμμα FERET (Face Recognition Technology), για να αξιολογήσει αλγορίθμους και να επιχορηγήσει την έρευνα για την αναγνώριση προσώπων. Όταν το πρόγραμμα τελείωσε το 1997, τα συστήματα αυτά ήταν απλά πρωτότυπα σε πανεπιστήμια και ερευνητικά κέντρα. Ως το τέλος της δεκαετίας 24 συστήματα ήταν διαθέσιμα. Η πιο σημαντική προσπάθεια αξιολόγησης συστημάτων αναγνώρισης προσώπου είναι το FRVT 2002 (Face Recognition Vendor Test), το οποίο είχε χορηγούς το Biometric Working Group της Αγγλίας, τις τελωνειακές αρχές της Αυστραλίας και το Γραφείο διαβατηρίων του Καναδά. Το επόμενο FRVT έγινε το 2006, το οποίο περιείχε τα αποτελέσματα του FRGC (Face Recognition Grand Challenge). Αυτή η "μεγάλη δοκιμασία" άρχισε το 2004 υπό την αιγίδα του Εθνικού Ινστιτούτου Προτυποποίησης και τεχνολογίας των ΗΠΑ.

Τα βιομετρικά συστήματα αναγνώρισης προσώπου, βασίζονται στη σύγκριση της πληροφορίας που εξάγεται από δυο ψηφιακές εικόνες. Πρέπει να δώσουμε σημασία στην διατύπωση της προηγούμενης πρότασης. Συγκρίνουμε πληροφορία που εξάγεται από δυο εικόνες και όχι δυο εικόνες. Κάποιες από τις τυπικές αιτίες που η άμεση σύγκριση των δυο φωτογραφιών δεν λειτουργεί είναι οι ακόλουθες:

- Προσθήκη ή αφαίρεση τριχών στο πρόσωπο (μουστάκι, μούσι κ.ά.)
- Αλλαγή στον τρόπο χτενίσματος
- Μακιγιάζ
- Διαφορετικές συνθήκες φωτισμού από την αρχική φωτογραφία

- Διαφορετική γωνία λήψης από την αρχική φωτογραφία
- Έκφραση
- Μαύρισμα
- Μαύροι κύκλοι στα μάτια

Επειδή ακριβώς δεν είναι δυνατόν να συγκρίνουμε άμεσα τις εικόνες εικονοστοιχείο (pixel) με εικονοστοιχείο, οι επιστήμονες προσπαθούν να βρουν τρόπους να αναπαραστήσουν με μαθηματικό τρόπο τις βασικές πληροφορίες μια φωτογραφίας. Παρακάτω ακολουθεί μια σύντομη περιγραφή των πιο σημαντικών τεχνικών που χρησιμοποιούνται στην αναγνώριση προσώπου.

Εικόνα 32. Αναπαράσταση με μαθηματικό τρόπο των βασικών χαρακτηριστικών ενός προσώπου

Elastic Bunch Graph Matching (EBGM)

Χρησιμοποιεί μεθόδους που πλησιάζουν σε εκείνες που χρησιμοποιούν τα ανώτερα θηλαστικά, συμπεριλαμβανομένου και του ανθρώπου, για να αναγνωρίσουν κάποιον. Η μέθοδος αυτή αναγνωρίζει τοπικά σημεία στο πρόσωπο, όπως γωνίες, το πάνω και το κάτω μέρος καθώς και το κέντρο των ματιών, και στη συνέχεια αυτά τα χαρακτηριστικά συγκρίνονται με ένα καινούριο σύνολο χαρακτηριστικό από μια νέα φωτογραφία. Η μέθοδος αυτή για να λειτουργήσει απαιτεί κάποια εκπαίδευση για να δουλέψει ικανοποιητικά με μια δεδομένη πισίνα προσώπων.

Principal Components Analysis (PCA)

Η μέθοδος αυτή χρησιμοποιεί γραμμικές αλγεβρικές τεχνικές για να μειώσει όσο γίνεται την πληροφορία που εξάγεται από την εικόνα, και στη συνέχεια συγκρίνει τις αποστάσεις των κανονικοποιημένων στοιχείων με τις αποστάσεις των στοιχείων της αρχικής εικόνας που έχουν υποστεί την ίδια επεξεργασία. Για να γίνει κατανοητό ας φανταστούμε τις μικρές γραμμές γέλιου στη γωνία του στόματος. Αν υπάρχουν παραπάνω από μια σε κάθε πλευρά, και έχουν πάνω κάτω το ίδιο μέγεθος και διεύθυνση, τότε μπορούν να αναπαρασταθούν με μια αντιπροσωπευτική γραμμή ή οποία είναι ο μέσος όρος των γραμμών. Αυτή η τεχνική επιτρέπει στο σύστημα να αναπαριστά την αναγκαία πληροφορία για να συγκριθούν δυο πρόσωπα, χρησιμοποιώντας πολύ λίγη πληροφορία, κάτι που είναι σημαντικό αν έχουμε πολλά πρόσωπα να αποθηκεύσουμε. Από την άλλη, η τεχνική αυτή μειονεκτεί εξαιτίας αυτής της κανονικοποίησης των χαρακτηριστικών, και τα μάτια, η μύτη και το στόμα θα πρέπει να είναι ευθυγραμμισμένα πριν εφαρμοσθεί η τεχνική.

Linear Discriminant Analysis (LDA)

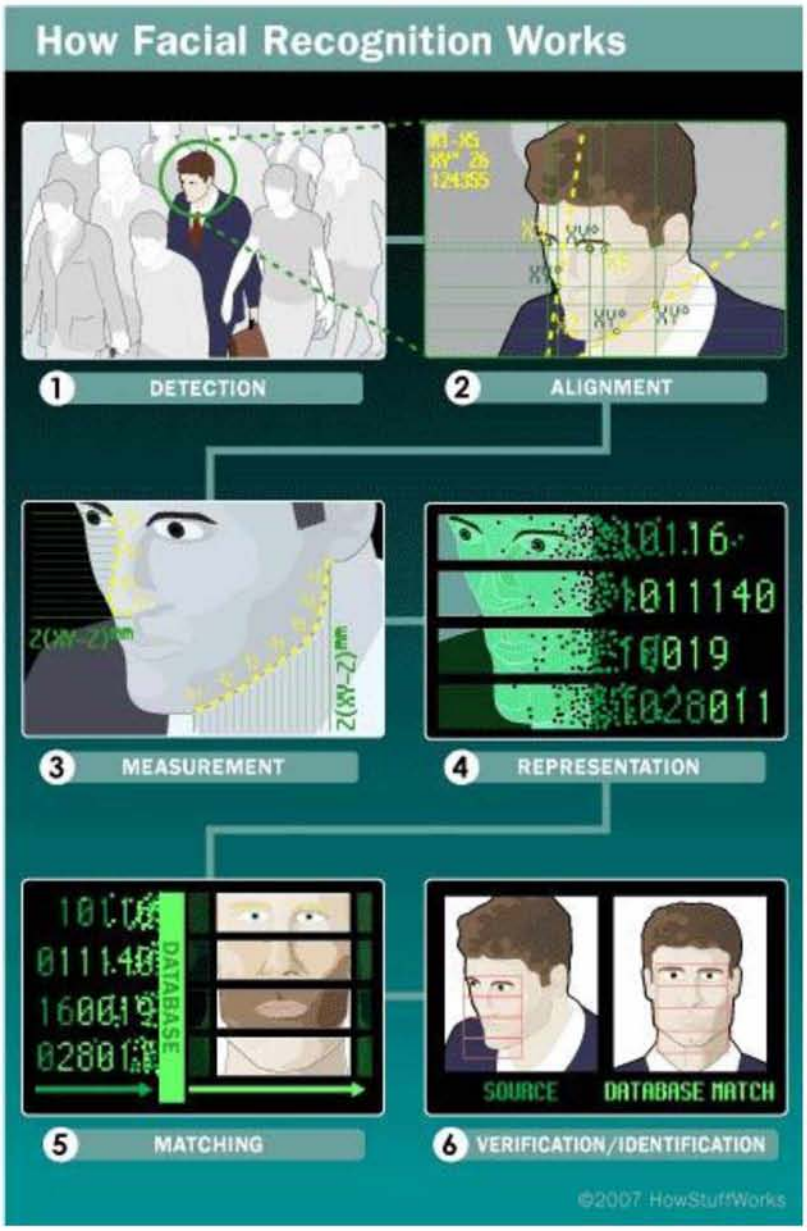
Η LDA είναι μια στατιστική τεχνική που επιχειρεί να παράγει μια καλή πρόβλεψη των χαρακτηριστικών που ένα δεδομένο πρόσωπο μπορεί να επιδείξει. Ουσιαστικά, η ιδέα είναι να "ξεφορτωθούμε" χαρακτηριστικά που διαφέρουν πολύ από δείγμα σε δείγμα και να επικεντρωθούμε σε εκείνα τα χαρακτηριστικά που παραμένουν σχετικά όμοια. Ταυτόχρονα, η LDA προσπαθεί να επιλέξει χαρακτηριστικά πρόβλεψης τα οποία μεγιστοποιούν τις διαφορές μεταξύ προσώπων που είναι γνωστό ότι δεν είναι τα ίδια. Όπως με όλα τα στατιστικά μοντέλα, η ακρίβεια της τεχνικής επηρεάζεται σημαντικά από το σύνολο των δειγμάτων που δίνονται για σύγκριση. Αν κάποια από τα δείγματα εικόνων προσώπου που χρησιμοποιούνται για να δημιουργηθεί η πρόβλεψη δεν είναι αντιπροσωπευτικά του προσώπου, αυτό θα έχει αρνητική επίδραση στην ικανότητα του συστήματος να αναγνωρίζει πρόσωπα.

Άσχετα με το ποια μέθοδος χρησιμοποιείται, η αναγνώριση προσώπου ακολουθεί πέντε βήματα.

1. Καταρχήν γίνεται λήψη μια φωτογραφίας του ατόμου. Αυτό μπορεί να γίνει είτε με ψηφιακή σάρωση μιας υπάρχουσας φωτογραφίας είτε με μια

ψηφιακή φωτογραφική μηχανή. Ένα βίντεο είναι μια γρήγορη ακολουθία στατικών εικόνων, οπότε μπορεί να χρειαστεί και αυτό ως πηγή.

2. Στη συνέχεια αναλαμβάνει την επεξεργασία της φωτογραφίας λογισμικό για να εντοπίσει τυχόν πρόσωπα. Είναι μια πολύ δύσκολη διαδικασία και συχνά χρησιμοποιούνται γενικευμένα πρότυπα για να καθοριστεί πως μοιάζει ένα πρόσωπο (δυο μάτια και ένα στόμα μέσα σε ένα οβάλ σχήμα) και εν τέλει να εντοπιστεί.
3. Μόλις το λογισμικό εντοπισμού προσώπου τελειώσει, τότε αρχίζει η ανάλυση. Χρησιμοποιούνται οι τεχνικές που προαναφέρθηκαν (EBGM, PCA, LDA) για να εξαχθούν τα χαρακτηριστικά. Η δημιουργία προτύπου είναι το αποτέλεσμα της διαδικασίας εξαγωγής χαρακτηριστικών. Ένα πρότυπο είναι ένα μειωμένο σύνολο δεδομένων που αναπαριστά τα μοναδικά χαρακτηριστικά ενός ατόμου.
4. Το τέταρτο βήμα είναι να συγκρίνουμε το πρότυπο που έχει παραχθεί με εκείνα σε μια βάση δεδομένων. Σε μια εφαρμογή αναγνώρισης, η διαδικασία αυτή μας δίνει ποσοστό ομοιότητας του προτύπου με τα αποθηκευμένα στη βάση. Σε μια εφαρμογή αυθεντικοποίησης το παραχθέν πρότυπο συγκρίνεται μόνο με το πρότυπο του ατόμου, την ταυτότητα του οποίου έχει ισχυριστεί το άτομο.
5. Στο πέμπτο και τελευταίο βήμα αποφασίζεται αν τα ποσοστά που παράχθηκαν στο προηγούμενο βήμα είναι αρκετά υψηλά για να υποδηλώσουν ένα ταίριασμα. Οι κανόνες σύμφωνα με τους οποίους ένα ταίριασμα είναι αποδεκτό, διαμορφώνονται από τον διαχειριστή του συστήματος, έτσι ώστε εκείνος να αποφασίζει πως θα συμπεριφέρεται το σύστημα αναγνώρισης ανάλογα με την πολιτική ασφαλείας (ποσοστά FAR, FRR).



Εικόνα 33. Διαδικασία αναγνώρισης προσώπου

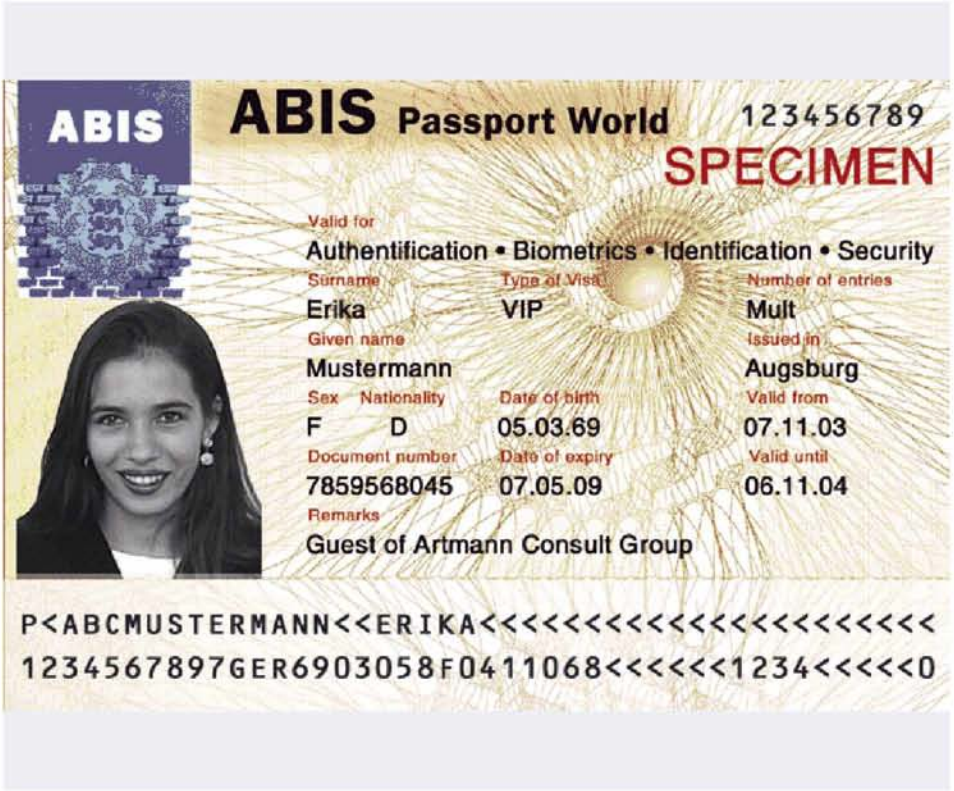
Που μπορεί να συναντήσουμε βιομετρικά συστήματα αναγνώρισης προσώπου.

Ίσως η πιο γνωστή χρήση ενός τέτοιου συστήματος ήταν το 2001 στο Super Bowl στη Φλόριντα των ΗΠΑ. Το Super Bowl ήταν στόχος τρομοκρατικής επίθεσης. Έτσι οι αρχές και η NSA, η εθνική υπηρεσία ασφαλείας των ΗΠΑ, αποφάσισαν να χρησιμοποιήσουν ένα σύστημα αναγνώρισης προσώπων. Θα έπρεπε να φωτογραφήσουν 100.000 άτομα καθώς θα έμπαιναν στο στάδιο και θα κυκλοφορούσαν στις εγκαταστάσεις του. Έτσι θα είχαν τη δυνατότητα με τη χρήση

της βιομετρίας, να συγκρίνουν τις εικόνες με μια βάση δεδομένων γνωστών εγκληματιών.

Οι υπέρμαχοι της ιδιωτικότητας αντιτάχθηκαν σε αυτή τη κίνηση. Οι αρχές όμως εξήγησαν ότι για να αναγνωριστεί κάποιος από το σύστημα θα έπρεπε πρώτα να έχει εγγραφεί σε αυτό. Το 99.9% των ανθρώπων που θα έμπαιναν στο γήπεδο δεν ήταν εγγεγραμμένοι σε κανένα τέτοιο σύστημα, πόσο μάλλον σε μια βάση δεδομένων εγκληματιών.

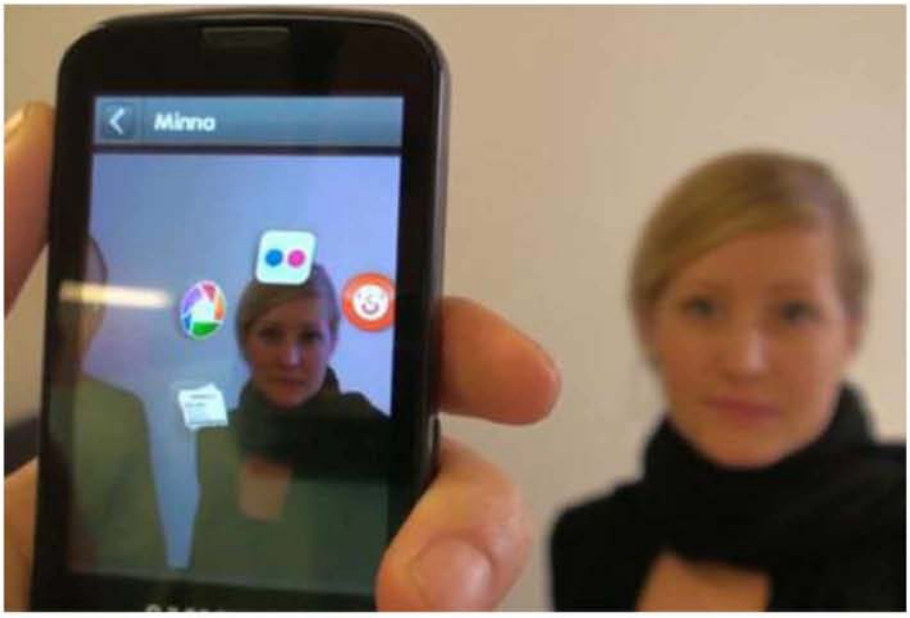
Η πιο σημαντική όμως κίνηση για την ανάπτυξη των συστημάτων αναγνώρισης προσώπου είναι η πρόταση της χρησιμοποίησης του προσώπου ως πρωτεύον βιομετρικό στα MRTDs (Machine Readable Travel Documents-Ταξιδιωτικά έγγραφα που διαβάζονται από μηχανές). Αυτή η πρόταση έγινε από την ICAO (International Civil Aviation Organization), μια οργάνωση των Ηνωμένων Εθνών, η οποία θέτει τις αρχές για τη διεθνή αεροπλοΐα και επιβλέπει τον σχεδιασμό των διεθνών αερομεταφορών για να εξασφαλίσει την ασφαλή ανάπτυξη του κλάδου. Η ICAO προτείνει πρότυπα (standards) και πρακτικές που αφορούν την επιθεώρηση πτήσεων, την αεροπλοΐα, την αποτροπή παράνομης παρέμβασης στη διαδικασία διάσχισης συνόρων.



Εικόνα 34. Διαβατήριο

Η δημοσιοποίηση προσωπικών μας φωτογραφιών σε site κοινωνικής δικτύωσης αποκτά νέο νόημα και νέους κινδύνους, σύμφωνα με το Popular Science. Η σουηδική εταιρεία The Astonishing Tribe (TAT) ετοιμάζει μια νέα εφαρμογή για κινητά τηλέφωνα με την οποία ο χρήστης θα μπορεί να φωτογραφίζει ένα πρόσωπο και με την μέθοδο της αναγνώρισης προσώπου να ταυτοποιεί τον φωτογραφούμενο με βάσει φωτογραφίες που έχει αναρτήσει σε σελίδες όπως το Facebook. Έτσι η εφαρμογή Recognizr σου δίνει την δυνατότητα να φωτογραφίζεις αγνώστους στον δρόμο, στο μετρό, σε ένα πάρτι και να μαθαίνεις το όνομα τους, αρκεί αυτοί να έχουν φωτογραφίες σε κάποιον λογαριασμό στα site κοινωνικής δικτύωσης.

Η διαδικασία συνδυάζει τις ήδη γνωστές τεχνολογίες του face recognition, computer vision, cloud computing και augmented reality (επαυξημένη πραγματικότητα). Η φωτογραφία του ατόμου-στόχου, μετατρέπεται σε 3D μοντέλο και στη συνέχεια ανεβαίνει στον server του Recognizr. Τη σκυτάλη παίρνει ένας cloud server ο οποίος με τη βοήθεια τεχνολογίας αναγνώρισης προσώπου αναζητά την φωτογραφία σε όλες τις γνωστές σελίδες κοινωνικής δικτύωσης και στέλνει πίσω στο χρήστη το όνομα του ατόμου και ένα link σχετικό με το προφίλ του. Η εφαρμογή δεν είναι ακόμη διαθέσιμη στο κοινό, έχει γίνει όμως γνωστό ότι θα λειτουργεί σε περιβάλλον iPhone και Android. (πηγή Cnet και PopSci)



Εικόνα35. Χρήση της εφαρμογής Recognizr

Το νέο τηλέφωνο της Sharp 904SH έρχεται με το νέο σύστημα ασφαλείας που έχει να κάνει με την αναγνώριση του προσώπου του κατόχου του. Το τηλέφωνο παρέχει την δυνατότητα του κλειδώματος σε όλα τα επίπεδα και την δυνατότητα να ξεκλειδώσει μόνο όταν αναγνωρίσει το πρόσωπο του κατόχου του μέσω ενός ειδικού αισθητήρα (OKI recognition sensor). Δεν χρειάζεται ούτε pin να χρησιμοποιεί κάποιος αφού το κλείδωμα και η αναγνώριση προσώπου γίνεται πριν την αναγνώριση της κάρτας sim και την εισαγωγή του pin.

Εικόνα 37. Κινητό τηλέφωνο με αναγνώριση προσώπου

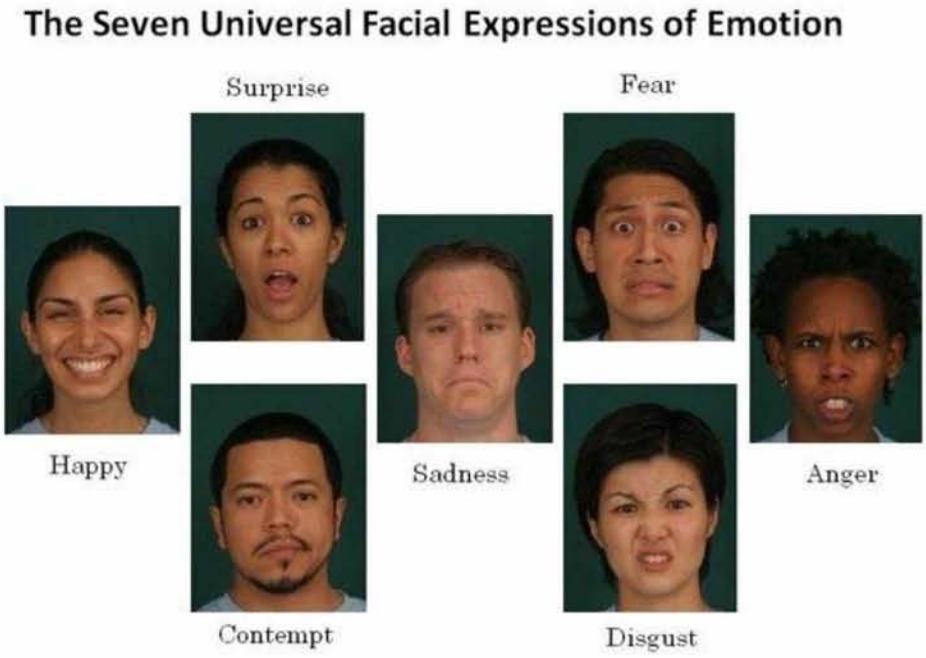
Ανάλυση εκφράσεων

Οι προσεγγίσεις σχετικά με την ανάλυση εκφράσεων διακρίνονται χονδρικά σε τρεις κατηγορίες ανάλογα με την πηγή της πληροφορίας που χρησιμοποιείται: (α) στατικές - χρήση εικόνων προσώπων που απεικονίζουν κάποια έκφραση, (β) ημιστατικές - χρήση δύο εικόνων, μια με το πρόσωπο σε ουδέτερη κατάσταση και μια με το πρόσωπο στη κορύφωση της έκφρασης και (γ) δυναμικές - χρήση ακολουθίας βίντεο στην οποία απεικονίζεται η εξέλιξη της έκφρασης.

Ο H. Shlosberg, καθηγητής ψυχολογίας στο πανεπιστήμιο Brown, στη μελέτη του “Three dimensions of emotion”, χρησιμοποίησε τρεις άξονες για την περιγραφή των συναισθημάτων: αποδοχής - απόρριψης A-R (attention - rejection), ευαρέσκειας - δυσαρέσκειας P-U (pleasantness - unpleasantness), και βαθμού ενεργοποίησης (level of activation). Για παράδειγμα συναισθήματα όπως η περιφρόνηση και η απέχθεια

χαρακτηρίζονται από υψηλή τιμή απόρριψης ενώ συναισθήματα όπως η οργή χαρακτηρίζονται από υψηλή τιμή δυσαρέσκειας.

Υπάρχουν έξι πρωτεύουσες εκφράσεις οι οποίες συνδέονται με αντίστοιχα συναισθήματα και οι οποίες μπορούν να αναγνωριστούν από τις μορφοποιήσεις του προσώπου. Οι εκφράσεις αυτές είναι χαρά, λύπη, έκπληξη, απέχθεια, οργή και φόβος. Πέρα από τις πρωτεύουσες εκφράσεις κατεγράφησαν πολλές άλλες οι οποίες όμως δεν είναι τόσο εύκολα ανιχνεύσιμες. Σήμερα οι βασικές εκφράσεις που παγκοσμίως εκφράζουν συναισθήματα είναι επτά: χαρά, λύπη, έκπληξη, απέχθεια, οργή, φόβος και περιφρόνηση.



Εικόνα 38. Οι 7 εκφράσεις προσώπου

Στο πεδίο των γραφικών για υπολογιστές και ιδιαίτερα στο animation έχουν εμφανιστεί πολλές εργασίες οι οποίες μοντελοποιούν τις εκφράσεις με βάση την κίνηση των μυών του προσώπου. Στην ανάλυση εκφράσεων τα χαρακτηριστικά του προσώπου είναι ιδιαίτερα σημαντικά και η αποτελεσματική ανίχνευση τους καθίσταται επιτακτική. Για το σκοπό αυτό οι εικόνες των προσώπων πρέπει να αρκετά υψηλής ανάλυσης και τα χαρακτηριστικά ευδιάκριτα.

Τα χαρακτηριστικά του προσώπου μπορούν να θεωρηθούν είτε στατικά - όπως για παράδειγμα το χρώμα του δέρματος - είτε αργά μεταβαλλόμενα - όπως υφή η

οποία μεταβάλλεται με την ανάπτυξη ρυτίδων - είτε κινούμενα - όπως οι βλεφαρίδες, τα φρύδια κοκ. Η ανίχνευση της θέση των χαρακτηριστικών αυτών από χρονικά σταθερές απεικονίσεις – φωτογραφίες - είναι ο στόχος των στατικών προσεγγίσεων της ανάλυσης εκφράσεων. Παρόλα αυτά υπάρχει ισχυρή ένδειξη ότι η αναγνώριση εκφράσεων από τον άνθρωπο στηρίζεται περισσότερο σε πληροφορία δυναμικής υφής παρά σε στατικές απεικονίσεις.

Σύμφωνα με μελέτη μια ομάδα ανθρώπων κλήθηκε να αναγνωρίσει εκφράσεις σε ακολουθίες βίντεο στις οποίες υπήρχαν φωτεινές κουκκίδες μόνο στις θέσεις των χαρακτηριστικών του προσώπου και οι υπόλοιπες περιοχές ήταν σκοτεινές. Από την συγκεκριμένη μελέτη προέκυψε ότι αναγνώριση πάνω από το επίπεδο τυχαιότητας ήταν εφικτή για όλες τις εκφράσεις, όταν χρησιμοποιούνταν ακολουθίες βίντεο ως πηγή πληροφορίας, ενώ με βάση τις στατικές εικόνες μόνο οι εκφράσεις "χαρά" και "λύπη" αναγνωρίστηκαν σε ποσοστό υψηλότερο από το επίπεδο τυχαιότητας. Δυστυχώς το συμπέρασμα έχει ουσιαστική αξία μόνο όσον αφορά την αντίληψη των εκφράσεων από τον άνθρωπο γιατί και η αναγνώριση εκφράσεων από τον υπολογιστή με βάση ακολουθίες βίντεο αντιμετωπίζει πολλά προβλήματα. Η ειδοποιός διαφορά μεταξύ ανθρώπου και υπολογιστή είναι η ακρίβεια εντοπισμού των προσώπων και των χαρακτηριστικών τους στο χώρο. Το ανθρώπινο οπτικό σύστημα είναι εξαιρετικά αποτελεσματικό στον τομέα αυτό. Αντίθετα στους υπολογιστές τα σφάλματα εντοπισμού του προσώπου και των χαρακτηριστικών του, λειτουργούν προσθετικά και σε πολλές περιπτώσεις καλύπτουν την ουσιαστική πληροφορία κίνησης που διατίθεται από τις ακολουθίες.

Το τελικό συμπέρασμα είναι ότι οι στατικές προσεγγίσεις οι οποίες είναι λιγότερο επιρρεπείς στον εντοπισμό των χαρακτηριστικών του προσώπου διατηρούν την αξία τους όσον αφορά την αναγνώριση των εκφράσεων. Από την άλλη πλευρά τα στάδια προεπεξεργασίας τα οποία αφορούν στον εντοπισμό του προσώπου, των βασικών χαρακτηριστικών του, όπως τα μάτια, μύτη, το στόμα κοκ, και σημείων στη περιοχή των χαρακτηριστικών αυτών είναι εξαιρετικά σημαντικά σε όλες τις περιπτώσεις. Οι δυναμικές προσεγγίσεις αντιμετωπίζουν επιπλέον και την πρόκληση της παρακολούθησης της κίνησης των χαρακτηριστικών με τεχνικές εκτίμησης κίνησης και μοντελοποίησης των μυών και των δράσεων τους.

Το FACS - Facial Action Coding System είναι ένα σύστημα ανατομικής περιγραφής το οποίο περιγράφει όλες τις οπτικά διαχωρίσιμες κινήσεις του προσώπου και στηρίζεται στον ορισμό των "μονάδων δράσης" action units (AU). Κάθε AU

αντιστοιχεί στην ταυτόχρονη δράση μιας ομάδας μυών οι οποίοι διαμορφώνουν μια συγκεκριμένη δράση στο πρόσωπο. Δεδομένου ότι αρκετοί μύες συμμετέχουν σε περισσότερες από μία AU δεν υπάρχει σαφής αντιστοιχία μυών και AU. Ένα σύνολο από 46 AU καλύπτει πλήρως τον έλεγχο των εκφράσεων ενώ άλλες 12 είναι υπεύθυνες για την θέση και κίνηση της ίριδας των ματιών. Το μοντέλο FACS χρησιμοποιήθηκε αποδοτικά για την σύνθεση εκφράσεων ενώ η χρήση του για ανάλυση εκφράσεων εξακολουθεί να ερευνάται. Ο Ekman και οι συνεργάτες του δημιούργησαν επίσης και ένα λεξικό, το EMFACS στο οποίο δηλώνονται οι AU οι οποίες περιγράφουν τις πρωτεύουσες εκφράσεις. Στη συνέχεια δημιούργησαν τη βάση FACSAID η οποία χρησιμοποιείται για τον υπολογισμό των συναισθηματικών εκφράσεων με βάση τις μετρήσεις των παραμέτρων του FACS. Το μοντέλο FACS ενέπνευσε και τη δημιουργία των παραμέτρων περιγραφής προσώπου και απόδοσης κίνησης προσώπου στο πλαίσιο του προτύπου ISO MPEG-4.

Η διαδικασία

Ενώ, για τους ανθρώπους, η ανίχνευση του προσώπου επιτυγχάνεται σχεδόν αβίαστα και η ερμηνεία των εκφράσεων σχετικά εύκολα, η ανάπτυξη ενός αυτόματου συστήματος που θα εντοπίζει και θα ταξινομεί με επιτυχία τις εκφράσεις του προσώπου, σε πραγματικό χρόνο, δεν είναι εύκολη υπόθεση. Το πρόβλημα μπορεί, γενικά, να αναλυθεί στα εξής βασικά στάδια:

- εντοπισμός του προσώπου μέσα στην εικόνα,
- επεξεργασία εικόνας/εξαγωγή της πληροφορίας για την έκφραση,
- κατηγοριοποίηση/αναγνώριση συναισθήματος.

Το σύστημα που θα προσεγγίζει τη λύση του παραπάνω προβλήματος περιγράφεται συνοπτικά από το μπλοκ διάγραμμα του Σχήματος. Η λειτουργία κάθε τμήματος παρουσιάζεται αναλυτικά στη συνέχεια.

Είσοδος

Στο σύστημα εισάγεται είτε μία στατική (μεμονωμένη) εικόνα είτε μία ακολουθία εικόνων (video), έγχρωμων ή στην κλίμακα του γκρι.

Εντοπισμός προσώπου

Σε αυτό το στάδιο διαχωρίζεται το πρόσωπο από το φόντο και αυτό μπορεί να γίνει είτε με την ανίχνευση της θέσης κάποιων σημείων αναφοράς, όπως οι ίριδες των ματιών και τα ρουθούνια, είτε με την εύρεση χρωματικών διαβαθμίσεων ή άλλων

χαρακτηριστικών, ενδεικτικών της "υφής" του προσώπου. Στις περισσότερες εφαρμογές μέχρι σήμερα, οι συνθήκες λήψης της εικόνας, όπως ο φωτισμός και ο προσανατολισμός του προσώπου, είναι ελεγχόμενες σε μεγάλο βαθμό, με το πρόσωπο να είναι κατά κανόνα σε εμπρόσθια όψη και στο κέντρο της εικόνας. Με αυτόν τον τρόπο, διευκολύνεται κατά πολύ η διαδικασία εντοπισμού του, αφού εξασφαλίζεται, καταρχήν, η παρουσία ενός προσώπου στην εικόνα και η a priori γνώση της θέσης του μέσα σε αυτήν κατά προσέγγιση. Αυτό, βέβαια, δεν μπορεί να επιτευχθεί σε πραγματικές εφαρμογές και αποτελεί μία σημαντική αδυναμία των περισσότερων συστημάτων, αφού πρακτικές δυσκολίες, όπως πρόσωπο σε κλίση, χαμηλός φωτισμός, συνωστισμός κ.ά., μπορούν να επιφέρουν μεγάλες αποκλίσεις στην επίδοση τους.

Επεξεργασία/Εξαγωγή χαρακτηριστικών

Πριν προχωρήσει κάποιος στην υλοποίηση αυτού του σταδίου, θα πρέπει, καταρχάς, να επιλέξει είτε την ολιστική (holistic) προσέγγιση, αντιμετωπίζοντας δηλαδή το πρόσωπο ως ένα ενιαίο σύνολο, είτε την αναλυτική/τοπική (analytic/localized) προσέγγιση, στην οποία το ενδιαφέρον επικεντρώνεται σε ένα σύνολο σημείων του προσώπου ή σε ένα σύνολο χαρακτηριστικών του (π.χ. μύτη, στόμα κλπ), είτε συνδυάζοντας τα παραπάνω σε μία υβριδική προσέγγιση.

Σε αυτό το τμήμα, ανάλογα με την προσέγγιση που χρησιμοποιήθηκε και τον τύπο της εισόδου, δημιουργείται μία υψηλότερης τάξης αναπαράσταση της εικόνας ή της ακολουθίας εικόνων του προσώπου, η οποία αντιπροσωπεύει γνωρίσματα χρήσιμα για την κατηγοριοποίηση, π.χ. γεωμετρία, υφή, παραμόρφωση, κίνηση, χρώμα, στατιστικές ή φασματικές ιδιότητες κ.ά. Σε αυτό το στάδιο, δηλαδή, μειώνονται οι διαστάσεις της εισόδου, διατηρώντας αλλά και αναδεικνύοντας τη σημαντική πληροφορία για την αναγνώριση. Στην πράξη, βέβαια, αυτό το τμήμα μπορεί να αποπροσανατολιστεί από λεπτομέρειες όπως ύπαρξη γυαλιών, τριχοφυΐας, μόνιμων ρυτίδων κλπ, γεγονός που πρέπει να ληφθεί σοβαρά υπόψη.

Κατηγοριοποίηση/Αναγνώριση συναισθήματος

Σε αυτό το τελευταίο τμήμα του συστήματος, η αναπαράσταση που προέκυψε στο προηγούμενο βήμα κατατάσσεται σε κάποιο από τα επτά "παγκόσμια" συναισθήματα ή σε κάποια από τις βασικές παραμορφώσεις του προσώπου (AUs), ανάλογα με το είδος της πληροφορίας που υφίσταται επεξεργασία. Φυσικά, το τμήμα του συστήματος που εκτελεί την κατάταξη πρέπει προηγουμένως να έχει

διαμορφωθεί σύμφωνα με δεδομένα εκπαίδευσης, δηλαδή εικόνες με γνωστή έκφραση ή κωδικοποιημένους συνδυασμούς AUs.

Συνήθως, το στάδιο της κατηγοριοποίησης είναι συνδυασμός ενός μηχανισμού σύγκρισης και ενός μηχανισμού απόφασης και υλοποιείται με τρεις βασικές μεθόδους:

- με βάση πρότυπα (template-based), συγκρίνοντας δηλαδή την εικόνα δοκιμής με τα πρότυπα και εξάγοντας αυτό με τη μεγαλύτερη ομοιότητα,
- με βάση νευρωνικά δίκτυα (Neural Network-based)
- με βάση κανόνες (rule-based) όταν πρόκειται για αντιστοίχιση ενός συνδυασμού AUs με ένα συναίσθημα.

Εφαρμογές

Ένα σύστημα με τα προαναφερθέντα χαρακτηριστικά, μπορεί να αποτελέσει τμήμα μιας πληθώρας εφαρμογών που θα αναβαθμίσουν την ποιότητα πολλών δραστηριοτήτων. Ενδεικτικά, αναφέρονται μερικοί τρόποι αξιοποίησης:

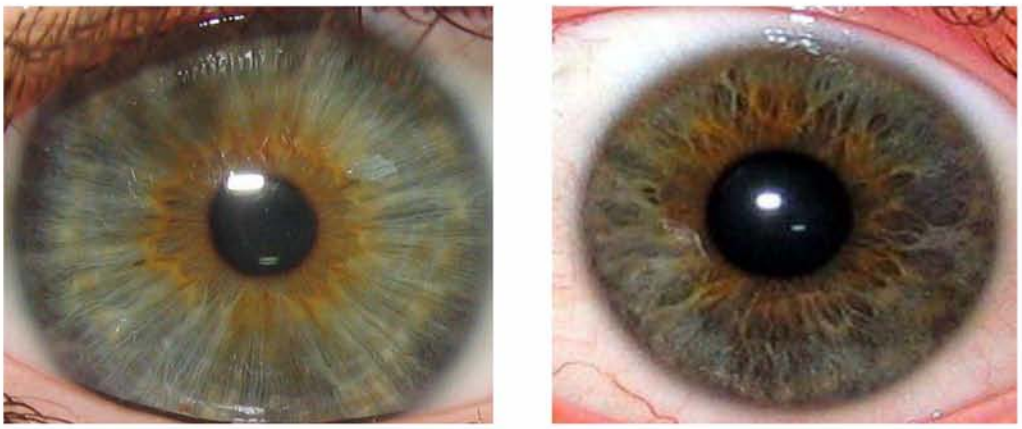
- Βοήθημα ανθρώπων με ιδιαιτερότητες, όπως ένα σύστημα ενίσχυσης της αναγνώρισης συναισθημάτων από άτομα με προβλήματα όρασης, ή ως ένα μέσο υποστήριξης και εκπαίδευσης παιδιών με αυτισμό.
- Πρόσθετο εργαλείο στην ιατρική φροντίδα, για παράδειγμα σε ένα ολοκληρωμένο σύστημα νοσηλευτικής παρακολούθησης χρόνιων ασθενών, ώστε να ανιχνεύεται και να αντιμετωπίζεται αναλόγως τυχόν αρνητική συναισθηματική αλλαγή (αίσθημα πανικού ή δυσανασχέτησης).
- Μέσο βελτίωσης των εφαρμογών εκπαίδευσης από απόσταση αλλά και των προγραμμάτων εκμάθησης μέσω υπολογιστή, δίνοντας τη δυνατότητα προσαρμογής του τρόπου και του ρυθμού διδασκαλίας σύμφωνα με τις αντιδράσεις του χρήστη.
- Λοιπές εφαρμογές: βελτίωση των λογισμικών προσωπικών υπολογιστών, των διαδραστικών ηλεκτρονικών παιχνιδιών, των μεθόδων μάρκετινγκ και διαφήμισης κ.ά.

Αναγνώριση ίριδας και αμφιβληστροειδούς

Αναγνώριση Ίριδας

Η αναγνώριση της ίριδας είναι η διαδικασία αναγνώρισης ενός ατόμου αναλύοντας το μοτίβο της ίριδας του ματιού. Η αυτόματη μέθοδος της αναγνώρισης ίριδας είναι σχετικά καινούρια, αφού υπάρχει μόλις από το 1994.

Η ίριδα είναι ένας μυς στο εσωτερικό του ματιού ο οποίος ρυθμίζει το μέγεθος της κόρης, ελέγχοντας την ποσότητα φωτός που εισέρχεται στο μάτι. Είναι το χρωματιστό τμήμα του ματιού και το χρώμα εξαρτάται από την ποσότητα μια χρωστικής ουσίας μέσα στο μυ που λέγεται μελατονίνη. Αν και ο χρωματισμός και η δομή της ίριδας είναι γενετικά συνδεδεμένα, οι λεπτομέρειες του μοτίβου δεν είναι. Αναπτύσσεται κατά τη διάρκεια της κύησης μέσα από μια διαδικασία αναδίπλωσης ιστών. Πριν τη γέννα, συμβαίνει εκφυλισμός, έχοντας σαν αποτέλεσμα να ανοίξει η κόρη και τα τυχαία και μοναδικά μοτίβα της ίριδας. Η πιθανότητα δυο άτομα να έχουν την ίδια ίριδα είναι $1:10^{52}$, γεγονός που καθιστά την ίριδα κατάλληλο βιομετρικό χαρακτηριστικό για αναγνώριση. Η ίριδα του ματιού περιέχει ένα πλούσιο και πολύπλοκο μωσαϊκό γραμμών και σχημάτων (υπάρχουν περίπου 200 τέτοια σημεία), τα οποία είναι μοναδικά για κάθε υποκείμενο. Οι μέθοδοι αναγνώρισης που βασίζονται στην ίριδα θεωρούνται από τις πλέον ακριβείς μεθόδους. Η έρευνα έχει δείξει ότι ο έλεγχος πρόσβασης με τη χρήση του αποτυπώματος της ίριδας εμφανίζει ποσοστά ακρίβειας μεγαλύτερα και από τις μεθόδους αναγνώρισης DNA.



Εικόνα 39. Ανθρώπινη ίριδα

Το 1936, ο οφθαλμίατρος Frank Burch πρότεινε τη μέθοδο χρησιμοποίησης μοτίβων ίριδας σαν μέθοδο αναγνώρισης ενός ατόμου. Το 1985, οι οφθαλμίατροι Leonard Flom και Aran Safir, απέδειξαν ότι δυο άτομα δεν μπορούν να έχουν την ίδια ίριδα και πήραν διάκριση για τη μέθοδο αυθεντικοποίησης μέσω ίριδας που επινόησαν το 1987. Ο Leonard Flom προσέγγισε τον John Daugman, ερευνητή στο Πανεπιστήμιο του Cambridge στο τμήμα επιστήμης υπολογιστών, για να αναπτύξουν έναν αλγόριθμο για να αυτοματοποιήσουν την αυθεντικοποίηση της ανθρώπινης ίριδας. Το 1993, η υπηρεσία Πυρηνικής Άμυνας των ΗΠΑ άρχισε να εργάζεται σε μια πρωτότυπη μονάδα, η οποία ολοκληρώθηκε επιτυχώς το 1995 χάρη στην συνδυασμένη προσπάθεια των Flom, Sarif και Daugman. Ο τελευταίος το 1994 πήρε την πατέντα για τους αλγόριθμους αυτόματης αναγνώρισης ίριδας, γεγονός που φρέναρε λίγο την ανάπτυξη της συγκεκριμένης τεχνολογίας. Το 2005 όμως η πατέντα η οποία κάλυπτε τη βασική ιδέα της αναγνώρισης ίριδας έληξε, δίνοντας την ευκαιρία σε εταιρίες της αγοράς να αναπτύξουν τους δικούς τους αλγόριθμους.

Διαδικασία

Συλλογή δεδομένων: Η πρώτη φάση της μεθόδου είναι να πάρουμε τη φωτογραφία του ματιού του ατόμου, χρησιμοποιώντας ψηφιακό αισθητήρα για μεγαλύτερη λεπτομέρεια.

Προεπεξεργασία εικόνας: Η εικόνα περνάει από μια πρώτη επεξεργασία φιλτραρίσματος για τη μείωση του θορύβου και των αντανακλάσεων όσο το δυνατόν περισσότερο, για να βελτιωθεί η ποιότητα του δείγματος. Σε αυτή τη φάση οριοθετείται η κόρη και η ίριδα για να τις ξεχωρίσουμε αργότερα.

Κατάτμηση εικόνας: Σε αυτή τη φάση η ίριδα εξάγεται από την εικόνα του ματιού. Ενοχλητικά χαρακτηριστικά όπως φρύδια και βλεφαρίδες απαλείφονται στο μέγιστο βαθμό και η ίριδα εξάγεται και κανονικοποιείται.

Εξαγωγή χαρακτηριστικών χρησιμοποιώντας στατιστικούς κανόνες: Η εξαγωγή των χαρακτηριστικών είναι πολύ σημαντική, γιατί σε αυτή τη φάση γίνεται η μετατροπή της δισδιάστατης εικόνας σε ένα σύνολο μαθηματικών παραμέτρων. Η ίριδα περιέχει σημαντικά, μοναδικά χαρακτηριστικά, όπως ρίγες, πιτσιλιές κ.ά. Τα χαρακτηριστικά αυτά αναφέρονται ως η υφή της ίριδας και εξάγονται χρησιμοποιώντας ποικίλους αλγόριθμους.

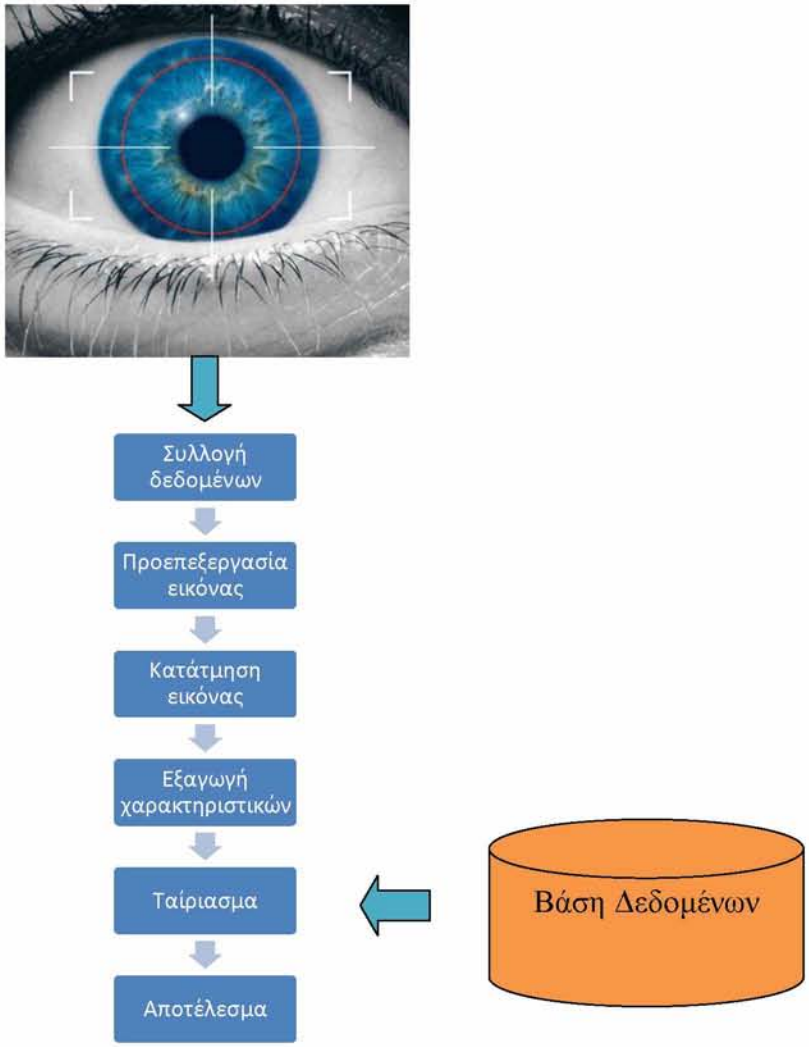
Ταίριασμα: Μόλις τα χαρακτηριστικά εξαχθούν, η εικόνα της ίριδας μεταμορφώνεται σε μια μοναδική αναπαράσταση σε ένα χαρακτηριστικό χώρο

(feature space). Για να παρθεί η απόφαση αποδοχής ή απόρριψης, υπολογίζεται η απόσταση μεταξύ του δείγματος και του προτύπου. Ένας τρόπος υπολογισμού αυτής της απόστασης είναι η Ευκλείδεια Απόσταση.

$$ED = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Όπου $F_1=(x_1, y_1)$ και $F_2=(x_2, y_2)$ είναι τα διανύσματα της εικόνας δείγματος και της εικόνας προτύπου στη βάση δεδομένων αντίστοιχα.

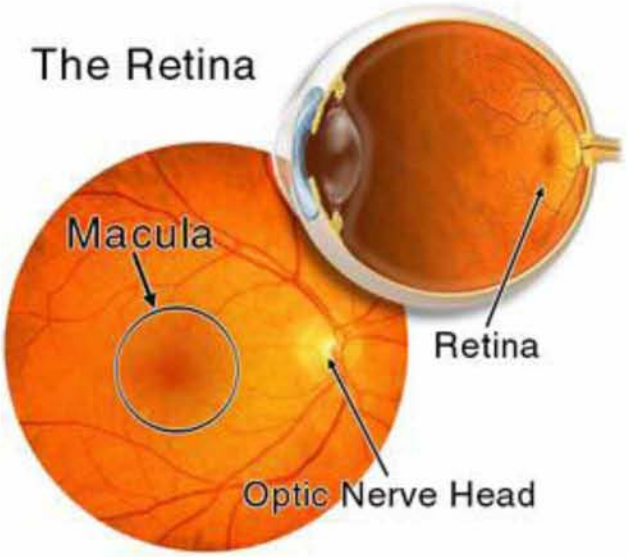
Αποτέλεσμα: Η απόφαση για την αποδοχή ή την απόρριψη του δείγματος επηρεάζεται από τις προδιαγραφές του συστήματος. Δηλαδή το κατώφλι αποδοχής του συστήματος είναι μια συγκεκριμένη τιμή Ευκλείδειας Απόστασης. Μέχρι αυτό το κατώφλι το αποτέλεσμα είναι αποδοχή, διαφορετικά απόρριψη.



Εικόνα 40.Διαδικασία αναγνώρισης ίριδας

Αναγνώριση αμφιβληστροειδούς

Λέγεται ότι "ο αμφιβληστροειδής είναι για το μάτι, ότι η ταινία για μια κάμερα". Αποτελείται από πολλαπλά επίπεδα αισθητήριων ιστών και εκατομμύρια φωτο-υποδοχείς, η λειτουργία των οποίων είναι να μετατρέπουν τις ακτίνες του φωτός σε ηλεκτρικά ερεθίσματα. Αυτά τα ερεθίσματα μεταφέρονται στον εγκέφαλο μέσω του οπτικού νεύρου, όπου και μετατρέπονται σε εικόνες. Υπάρχουν δυο ειδών φωτο-υποδοχείς: τα ραβδία (rods) και οι κώνοι (cones). Οι κώνοι είναι υπεύθυνοι για να βλέπουμε τα διάφορα χρώματα και είναι περίπου 6 εκατομμύρια. Τα ραβδία, περίπου 125 εκατομμύρια, διευκολύνουν τη νυχτερινή και περιφερειακή όραση. Το μοτίβο των αιμοφόρων αγγείων είναι εκείνο που αποτελεί τη βάση για τη χρησιμοποίηση του αμφιβληστροειδούς ως βιομετρικό χαρακτηριστικό, κατάλληλο για αναγνώριση ενός ατόμου.



Εικόνα 41. Ανθρώπινος αμφιβληστροειδής

Εξαιτίας της θέσης του στο εσωτερικό του ματιού, ο αμφιβληστροειδής δεν έρχεται σε επαφή με το περιβάλλον, οπότε σαν βιομετρικό είναι πολύ σταθερό. Οι κόκκινες γραμμές αναπαριστούν τα αιμοφόρα αγγεία, ενώ το κίτρινο τμήμα καταδεικνύει το σημείο του οπτικού δίσκου, το σημείο δηλαδή που ενώνεται το οπτικό νεύρο με τον αμφιβληστροειδή.

Υπάρχουν δυο μελέτες που έχουν επιβεβαιώσει τη μοναδικότητα του μοτίβου των αιμοφόρων αγγείων στον αμφιβληστροειδή. Η πρώτη δημοσιεύθηκε από τους Carleton Simon και Isodore Goldstein Φαρμακευτικό Ημερολόγιο της Νέας Υόρκης το 1935 και περιγράφει πως κάθε αμφιβληστροειδής περιέχει μοναδικό μοτίβο

αιμοφόρων αγγείων. Πρότειναν επίσης τη χρησιμοποίηση φωτογραφιών αυτών των μοτίβων ως μέσο αναγνώρισης. Η δεύτερη μελέτη έγινε το 1950 από τον Paul Tower. Ανακάλυψε λοιπόν, ότι ακόμα και ανάμεσα σε δυο πανομοιότυπα δίδυμα, ο αμφιβληστροειδής είναι διαφορετικός.

Η πρώτη εταιρεία που ασχολήθηκε με την έρευνα, ανάπτυξη και κατασκευή συσκευών σάρωσης αμφιβληστροειδούς, ήταν η EyeDentify Inc. Η εταιρεία δημιουργήθηκε το 1976 και οι πρώτες συσκευές σάρωσης αμφιβληστροειδούς ονομάζονταν "fundus cameras". Ενώ αρχικά προορίζονταν μόνο από οφθαλμίατρους, τροποποιημένες εκδοχές τους χρησιμοποιήθηκαν για τη φωτογράφιση εικόνων αμφιβληστροειδούς. Η συσκευή όμως είχε πολλά μειονεκτήματα. Καταρχήν ο εξοπλισμός ήταν πολύ ακριβός και δύσκολα μπορούσε κάποιος να το χειριστεί. Το φως που χρησιμοποιείται για το φωτισμό του αμφιβληστροειδούς θεωρούταν πολύ φωτεινό και ενοχλητικό για το χρήστη.

Η έρευνα τελικά απέδωσε καρπούς. Το 1981 αποκαλύφθηκε το πρωτότυπο. Η συσκευή χρησιμοποιούσε υπέρυθρο φως για το φωτισμό των αιμοφόρων αγγείων. Το πλεονέκτημα του υπέρυθρου φωτός είναι ότι τα αιμοφόρα αγγεία μπορούν να απορροφήσουν τέτοιου είδους φως, πολύ πιο γρήγορα από οποιοδήποτε άλλο ιστό. Το φως που αντανακλάται, το επεξεργάζεται η συσκευή.

Η συνολική διαδικασία μπορεί να σπάσει σε τρεις υποδιεργασίες:

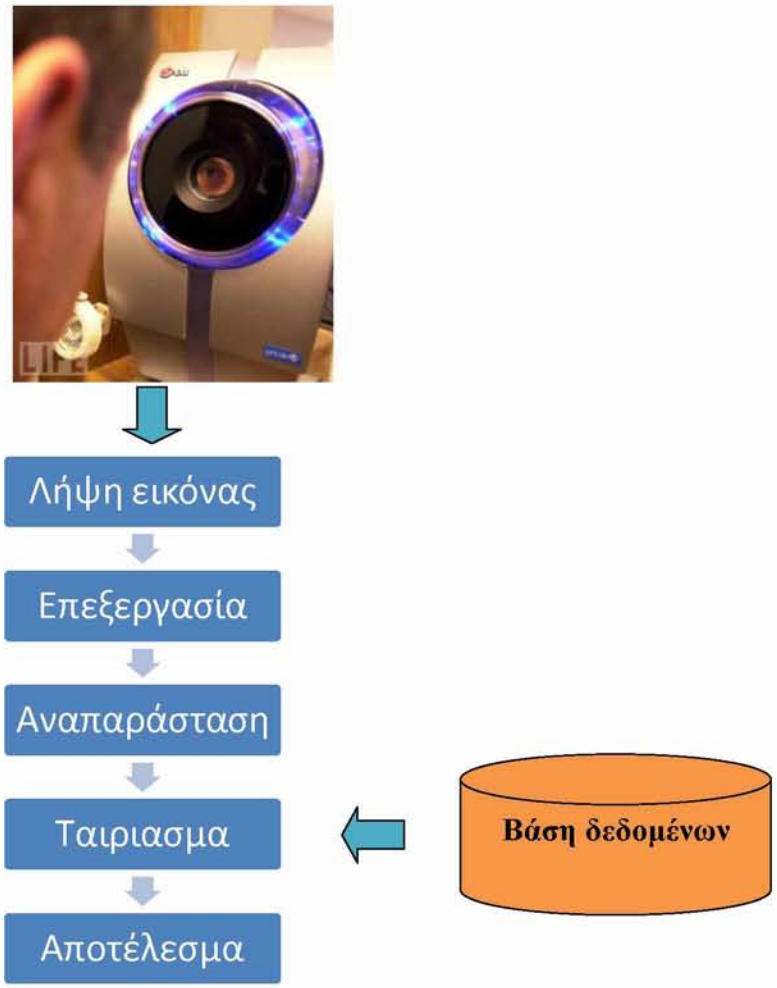
1. Λήψη εικόνας και επεξεργασία. Αυτή η υποδιεργασία περιέχει τη λήψη της εικόνας του αμφιβληστροειδούς και τη μετατροπή της σε ψηφιακή μορφή.
2. Αναπαράσταση: Τα μοναδικά χαρακτηριστικά του αμφιβληστροειδούς παρουσιάζονται ως πρότυπο.
3. Ταίριασμα: Ένας υπολογιστής χρησιμοποιείται για να αναγνωρίσει το χρήστη.

Η διαδικασία της εγγραφής και της αυθεντικοποίησης / αναγνώρισης σε ένα τέτοιο σύστημα είναι η ίδια με τη διαδικασία που χρησιμοποιείται και στα άλλα βιομετρικά συστήματα (λήψη και επεξεργασία εικόνας, εξαγωγή χαρακτηριστικών, δημιουργία προτύπου). Η λήψη της εικόνας και η φάση επεξεργασίας είναι οι πιο πολύπλοκες. Η ταχύτητα και η ευκολία της υποδιεργασίας αυτής, εξαρτάται από τη συνεργασία του χρήστη. Για να γίνει η σάρωση, ο χρήστης θα πρέπει να τοποθετήσει το μάτι του πολύ κοντά στο φακό. Για τη διασφάλιση της ποιότητας της εικόνας θα πρέπει ο χρήστης να παραμείνει ακίνητος. Ο χρήστης βλέπει ένα πράσινο φως σε ένα

άσπρο φόντο. Μόλις ο σαρωτής ενεργοποιηθεί, το πράσινο φως κινείται κυκλικά διαγράφοντας ένα πλήρη κύκλο. Ανάλογα με τη συνεργασία του χρήστη, η διαδικασία αυτή η μπορεί να πάρει έως και ένα λεπτό. Πολύ μεγαλύτερος χρόνος από τα άλλα βιομετρικά χαρακτηριστικά.

Το επόμενο στάδιο περιλαμβάνει την εξαγωγή δεδομένων. Ένα πολύ μεγάλο πλεονέκτημα την χρησιμοποίησης του αμφιβληστροειδούς αποδεικνύεται. Καθώς οι γενετικοί παράγοντες δεν υπαγορεύουν το μοτίβο των αιμοφόρων αγγείων, ο αμφιβληστροειδής περιέχει μια ποικιλία μοναδικών χαρακτηριστικών. Αυτό επιτρέπει τη λήψη έως και 400 μοναδικών σημείων που μπορούν να εξαχθούν, τη στιγμή που κάποια άλλα βιομετρικά, όπως η αναγνώριση δακτυλικών αποτυπωμάτων, παρέχουν μόνο 30-40.

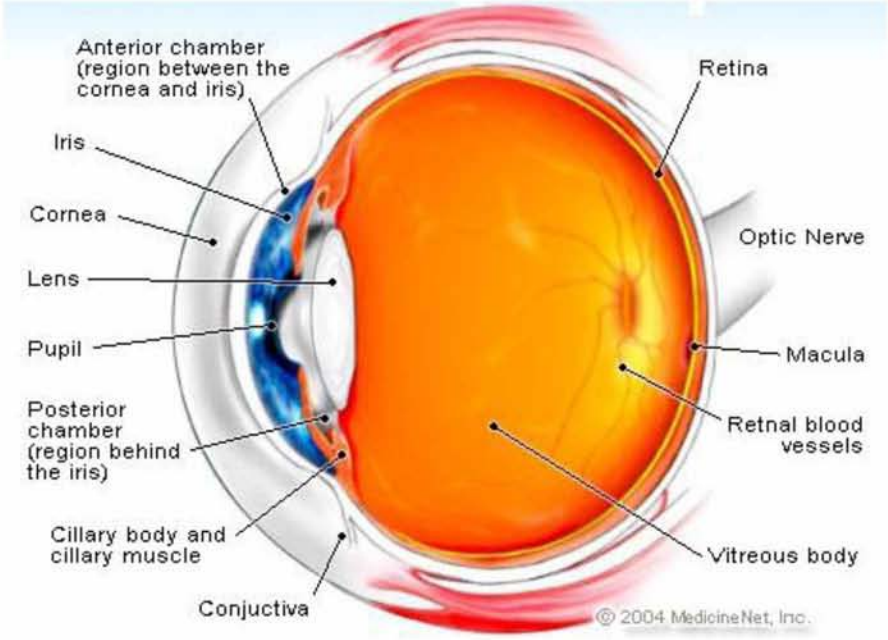
Κατά τη διάρκεια της τελευταίας υποδιεργασίας, το μοναδικό μοτίβο μετατρέπεται σε πρότυπο εγγραφής. Με μόλις 96 bytes μέγεθος, το πρότυπο αμφιβληστροειδούς θεωρείται ένα από τα μικρότερα βιομετρικά πρότυπα.



Εικόνα 42. Αναγνώριση αμφιβληστροειδούς

Αναγνώριση ίριδας έναντι αναγνώρισης αμφιβληστροειδούς

Η αναγνώριση ίριδας χρησιμοποιεί το μυ της ίριδας ενώ η αναγνώριση αμφιβληστροειδούς χρησιμοποιεί το μοναδικό μοτίβο των αιμοφόρων αγγείων στο πίσω μέρος του ματιού.



Εικόνα 43. **Η δομή του ματιού**

Και οι δυο τεχνικές περιλαμβάνουν λήψη μια εικόνας πολύ υψηλής ποιότητας της ίριδας ή του αμφιβληστροειδούς. Κατά τη λήψη των εικόνων αυτών, είναι αναγκαία μια μορφή φωτισμού. Χρησιμοποιείται και στις δυο τεχνικές NIR φως (near infrared). Το σημαντικότερο κοινό χαρακτηριστικό των δυο μεθόδων είναι η προσοχή κατά τη διάρκεια του σχεδιασμού. Αυτό γιατί η ασφάλεια του ματιού κατά τη διάρκεια της ακτινοβόλησης του με NIR φως είναι πρωταρχικής σημασίας.

Εφαρμογές

Ένα σύστημα αναγνώρισης ίριδας ή αμφιβληστροειδούς, μπορεί να αποτελέσει τμήμα μιας πληθώρας εφαρμογών που θα αναβαθμίσουν την ποιότητα πολλών δραστηριοτήτων.

- Φυσική πρόσβαση σε χώρους αυξημένης ασφάλειας.
- Λογική πρόσβαση σε συστήματα (ATM) και υπολογιστές.
- Έλεγχο πρόσβασης στα σύνορα και στα αεροδρόμια (σύστημα IRIS).

- Έλεγχος και πρόληψη του κοινού από κολλητικές ασθένειες. (Ασθένειες όπως η ελονοσία, η σύφιλη, η Νόσος του Lyme ή Μπορρελίωση επηρεάζουν τα μάτια)

Εικόνα 44. Έλεγχος πρόσβασης στα σύνορα

Εικόνα 45. CANPAS(air Canada)

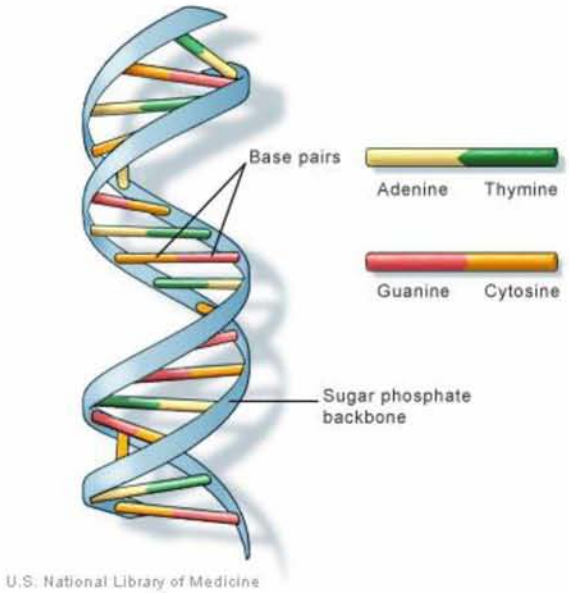
Εικόνα 46. Κινητό τηλέφωνο με αναγνώριση ίριδας

Iris Recognition Immigration System (IRIS)

Το σύστημα IRIS είναι ένα μέσο ελέγχου πρόσβασης συνόρων, που επιτρέπει σε εγγεγραμμένους επιβάτες να εισέρχονται στο Ηνωμένο Βασίλειο γρήγορα μέσω αυτόματων θυρών σε συγκεκριμένα αεροδρόμια. Χρησιμοποιεί ένα σύστημα αναγνώρισης ίριδας για την αυθεντικοποίηση των επιβατών. Η εγγραφή στο σύστημα IRIS χρειάζεται περίπου 5-10 λεπτά. Ένας εγγεγραμμένος ταξιδιώτης που εισέρχεται στο Ηνωμένο Βασίλειο, μπορεί να περάσει μια IRIS θύρα σε περίπου 20 δευτερόλεπτα. Έτσι οι ταξιδιώτες που μετακινούνται συχνά γλιτώνουν πολύ χρόνο και τα αεροδρόμια κερδίζουν σε εργατοώρες, αφού πλέον δε χρειάζεται τόσο προσωπικό και τόση ώρα για την αυθεντικοποίηση ενός ατόμου. Το συγκεκριμένο σύστημα ήδη χρησιμοποιείται σε αεροδρόμια όπως του Heathrow, του Manchester και του Birmingham.

Αναγνώριση DNA

Το δεοξυριβονουκλεϊκό οξύ (Deoxyribonucleic acid - DNA) είναι ένα νουκλεϊκό οξύ που περιέχει τις γενετικές πληροφορίες που καθορίζουν τη βιολογική ανάπτυξη όλων των κυτταρικών μορφών ζωής και των περισσοτέρων ιών. Το DNA συνήθως εντοπίζεται με τη μορφή μιας διπλής έλικας.



Εικόνα 46. Το ανθρώπινο γωνιδίωμα (DNA)

Η ανακάλυψη της δομής του DNA πραγματοποιήθηκε το 1953 από τους Τζέιμς Γουάτσον και Φράνσις Κρικ. Από πολλούς η ανακάλυψη της διπλής έλικας του DNA θεωρείται ως η μεγαλύτερη βιολογική ανακάλυψη του 20ου αιώνα. Για τη συνεισφορά τους στη μελέτη της δομής του DNA, οι Γουάτσον και Κρικ μοιράστηκαν το 1962 το βραβείο Νόμπελ με τον Μορίς Γουίλκινς, ο οποίος εργάστηκε προς την ίδια κατεύθυνση.

Δείγμα από το γενετικό υλικό χρησιμοποιείται για τη δημιουργία ενός DNA αποτυπώματος ή DNA προφίλ. Η δημιουργία ενός DNA προφίλ είναι μια τεχνική που χρησιμοποιείται από επιστήμονες της εγκληματολογίας, για να τους βοηθήσουν στη διαδικασία αυθεντικοποίησης ενός ατόμου. Είναι ένα κρυπτογραφημένο σύνολο αριθμών που αναπαριστούν το DNA ενός ατόμου.

Θα πρέπει να γνωρίζουμε όμως κάποια βασικά πράγματα για το DNA:

- Μόνο το 2-3% της γενετικής ακολουθίας αναπαριστά το γνωστό γενετικό υλικό.
- Σχεδόν το 70% της ακολουθίας αποτελείται από μη κωδικοποιημένες περιοχές, των οποίων τη λειτουργία δε γνωρίζουμε.

Η αυθεντικοποίηση με τη χρήση του γενετικού υλικού βασίζεται σε τεχνικές που χρησιμοποιούν τις μη κωδικοποιημένες, διπλού άξονα, ταυτολογικές περιοχές. Το DNA γενικότερα δεν θεωρείται, από μια μερίδα επιστημόνων, ως μια βιομετρική

τεχνολογία αναγνώρισης, κυρίως γιατί δεν είναι ακόμα αυτοματοποιημένη διαδικασία, αφού χρειάζονται ώρες για τη δημιουργία ενός DNA αποτυπώματος. Όμως, εξαιτίας της τεράστιας ακρίβειας που παρέχει και της μονιμότητας μέσα στο χρόνο ζωής ενός ατόμου, η έρευνα των βιομετρικών δεν θα μπορούσε να το αγνοήσει.

Το στατιστικό δείγμα δείχνει ότι η πιθανότητα δυο άτομα να έχουν το ίδιο DNA προφίλ είναι 1 στα 6 δισεκατομμύρια. Παρόλα αυτά, η χρησιμοποίηση τεχνικών DNA για την αναγνώριση δυο πανομοιότυπων διδύμων, θα μας έδινε 100% λανθασμένη αποδοχή (πολύ υψηλό FAR). Για το λόγο αυτό μπορεί να χρησιμοποιηθεί ένας συνδυασμός βιομετρικών τεχνικών. Η πιθανότητα πανομοιότυπων διδύμων είναι 1 στις 250 ή 0,4%. Για όλο τον υπόλοιπο πληθυσμό το DNA είναι μοναδικό και μπορεί εύκολα να χρησιμοποιηθεί ως βιομετρικό χαρακτηριστικό.

Η συλλογή του γενετικού υλικού στο παρελθόν θεωρούταν ως "δειγματοληπτική εισβολή" (θα έπρεπε να τρυπήσουμε το δάκτυλο του χρήστη για να πάρουμε δείγμα από το αίμα του). Όμως οι δειγματοληπτικές μέθοδοι έχουν εξελιχθεί για να απαλείψουν αυτό το φόβο. Πλέον η δειγματοληψία μπορεί να γίνει από το σάλιο ή από τα επιδερμικά κύτταρα του χρήστη, τα οποία λαμβάνονται με κολλητική ταινία από τον πήχη.

Το κύριο πρόβλημα όμως με το γενετικό υλικό είναι ότι περιέχει ευαίσθητες πληροφορίες για τη γενετική και την κατάσταση υγείας του χρήστη. Έτσι, οποιαδήποτε κακή χρήση της συγκεκριμένης πληροφορίας, μπορεί να αποκαλύψει κληρονομικούς παράγοντες ή διαταραχές στην υγεία. Το DNA προφίλ όμως, είναι απλά μια ένα σύνολο αριθμών, οπότε δεν δίνει πληροφορίες. Στη εγκληματολογία, η επιλογή των σημείων αναφοράς για την εξέταση του DNA, γίνεται έτσι ώστε να είναι μακριά από γονίδια. Με αυτό τον τρόπο, δεν μπορεί να γίνει συσχετισμός με καμία γενετική ασθένεια.

Η δημιουργία ενός γενετικού αποτυπώματος περιγράφηκε πρώτη φορά το 1985 από έναν Άγγλο γενετιστή, τον Alec Jeffreys. Ανακάλυψε ότι ορισμένες περιοχές του γενετικού υλικού, περιέχουν επαναλαμβανόμενες ακολουθίες. Επίσης διέκρινε ότι ο αριθμός αυτών των επαναλαμβανόμενων περιοχών διέφεραν από άνθρωπο σε άνθρωπο. Αναπτύσσοντας λοιπόν μια τεχνική για τη μελέτη των διαφόρων μηκών αυτών των ακολουθιών, ο Jeffreys έδωσε τη δυνατότητα για τη διεξαγωγή αυθεντικοποίησης σε ανθρώπους. Αυτές οι επαναλαμβανόμενες περιοχές ονομάστηκαν VNTRs (Variable Number of Tandem Repeats). Η τεχνική του ονομάστηκε RFLP (Restriction Fragment Length Polymorphism), γιατί απαιτούσε τη

χρήση ενός περιοριστικού ενζύμου που έκοβε τις περιοχές του DNA γύρω από τα VNTRs. Χρησιμοποιήθηκε για πρώτη φορά στον έλεγχο μεταναστών και στην εγκληματολογία για τη διαλεύκανσης μια υπόθεσης βιασμού και δολοφονίας δυο γυναικών.

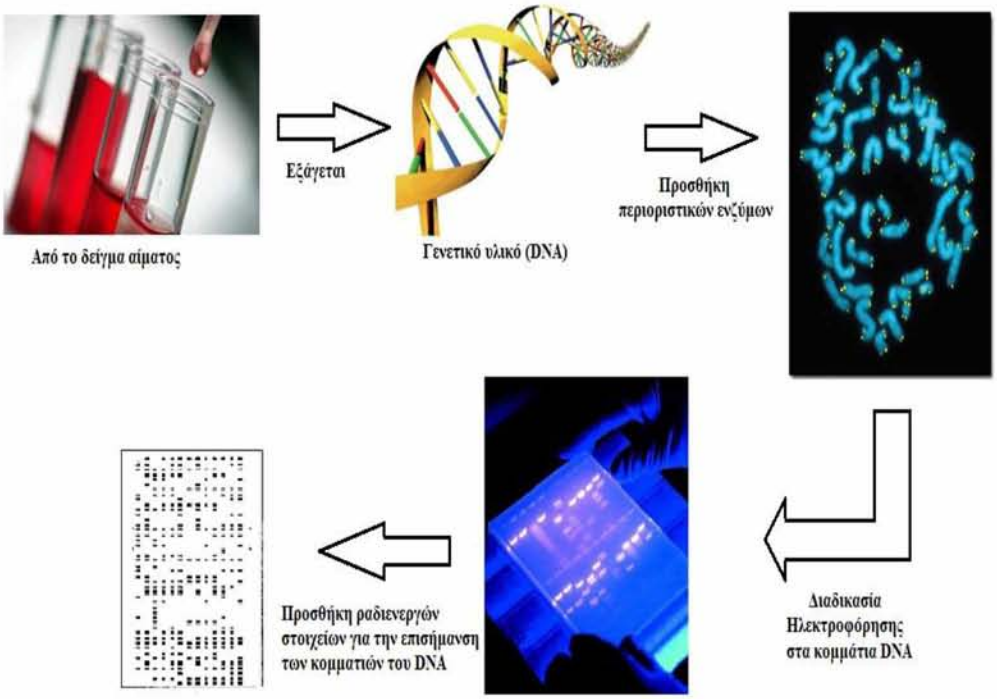
Οι δυο κοπέλες 15 και 17 χρονών, βιάστηκαν και δολοφονήθηκαν σε διαφορετικά μέρη η μια το 1983 και η άλλη το 1986. Κύριος ύποπτος για τα εγκλήματα ήταν ένας δεκαεπτάχρονος, ο Richard Backland. Καταδικάστηκε σε πολυετή κάθειρξη. Οι δικηγόροι του όμως, γνωρίζοντας τη μελέτη του Jeffreys, άσκησαν έφεση και ζήτησαν να γίνει έλεγχος DNA. Πήραν λοιπόν δείγμα από το σπέρμα του Backland και από τις δυο κοπέλες και τα συνέκριναν. Το πόρισμα ήταν πως οι κοπέλες βιάστηκαν από τον ίδιο άνδρα, αλλά όχι από τον Backland. Αφέθηκε ελεύθερος και οι αρχές άρχισαν πάλι τις έρευνες. Με τη βοήθεια της υπηρεσίας FSS (Forensic Science Service) ανακάλυψαν τελικά τον ένοχο, ο οποίος ήταν ο Colin Pitchfork. Καταδικάστηκε σε 30 χρόνια κάθειρξη.

Διαδικασία DNA fingerprinting

Η δημιουργία ενός γενετικού αποτυπώματος είναι μια εργαστηριακή διεργασία που απαιτεί τέσσερα βήματα:

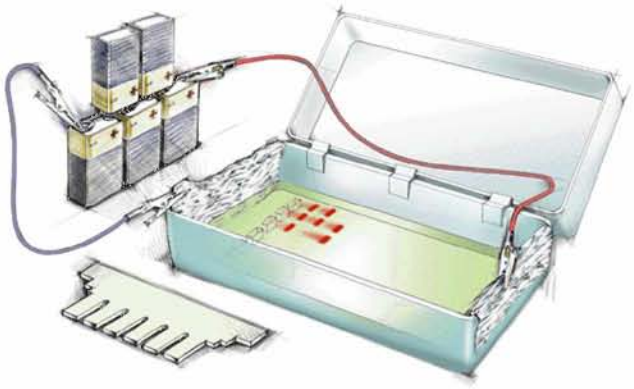
1. Απομόνωση του DNA: Το γενετικό υλικό πρέπει να εξαχθεί από τα κύτταρα ή τους ιστούς του ατόμου. Μόνο μια μικρή ποσότητα ιστού είναι αναγκαία. Για παράδειγμα η ποσότητα γενετικού υλικού στη βάση μιας τρίχας είναι συνήθως αρκετή.
2. Κατάτμηση, ορισμός μεγέθους και κατηγοριοποίηση: Ειδικά ένζυμα που ονομάζονται περιοριστικά ένζυμα χρησιμοποιούνται για να “κόψουν” το DNA σε συγκεκριμένες θέσεις. Στη συνέχεια μέσω μιας διαδικασίας κοσκινίσματος κατηγοριοποιούνται ανάλογα με το μέγεθος τους. Η διαδικασία ονομάζεται ηλεκτροφόρηση (electrophoresis). Τα κομμάτια του γενετικού υλικού τοποθετούνται πάνω στη μια πλευρά μιας πλάκας με πολτώδη μάζα και στις άκρες της εφαρμόζεται τάση. Τα κομμάτια φορτίζονται και η τάση εφαρμόζεται με τέτοιο τρόπο έτσι ώστε τα κομμάτια του γενετικού υλικού να μετακινούνται προς την άλλη κατεύθυνση. Τα μικρότερα κομμάτια κινούνται πιο γρήγορα από τα μεγαλύτερα και έτσι επιτυγχάνεται ο διαχωρισμός.

3. Μεταφορά του DNA στο νάιλον: Τα κομμάτια του γενετικού υλικού μεταφέρονται σε ένα νάιλον φύλλο τοποθετώντας το πάνω στο gel που περιέχει το γενετικό υλικό.
4. Ραδιενεργός χρωματισμός: Προσθέτουμε ραδιενεργά ή χρωματισμένα στοιχεία στο νάιλον και παράγεται ένα μοτίβο που ονομάζεται γενετικό αποτύπωμα. Θα μπορούσαμε να το παρομοιάσουμε με ένα barcode.



Εικόνα 47. Διαδικασία δημιουργίας γενετικού αποτυπώματος

Εικόνα 48. Συλλογέας DNA (Σάλιο)



Εικόνα 49. Συσκευή ηλεκτροφόρησης

Διαδικασία

Η εγγραφή σε ένα σύστημα DNA είναι πάντα εφικτή. Ο καθένας έχει DNA κάθε στιγμή. Επιπρόσθετα, το γενετικό υλικό επιτρέπει την εγγραφή μόλις το άτομο γεννηθεί. Άρα ένα από τα κυριότερα πλεονεκτήματά του, είναι ότι η εγγραφή παρουσιάζει μηδενικό (0%) ποσοστό αποτυχίας εγγραφής (FTE-Failure To Enroll).

Λήψη δείγματος: Συλλογή του γενετικού υλικού μπορεί να γίνει με πολλούς τρόπους, όπως λήψη λίγων σταγόνων αίματος από το χέρι, λίγο σάλιο ή ένα ειδικό αυτοκόλλητο στο χέρι του ατόμου. Το σημαντικότερο είναι η φύλαξη και αποθήκευση του γενετικού υλικού, γιατί μπορεί να μολυνθεί ή να διασπαστεί. Αυτό μπορεί να γίνει είτε από την υγρασία, είτε από έκθεση σε έντονο φως, είτε από τη θερμοκρασία. Οπότε η καλύτερη μέθοδος φύλαξης είναι να το ψύξουμε άμεσα και να το αποθηκεύσουμε.

Εξαγωγή χαρακτηριστικών: Μετατροπή του δείγματος σε πρότυπο. Όπως περιγράφηκε προηγουμένως, Το δείγμα του γενετικού υλικού μας παρέχει το γενετικό αποτύπωμα, μέσω της διαδικασίας της ηλεκτροφόρησης. Η ψηφιοποίηση του αποτελέσματος γίνεται με μια ψηφιακή μηχανή, η οποία παίρνει την εικόνα του αποτυπώματος για να συγκριθεί αργότερα με εικόνες άλλων γενετικών αποτυπωμάτων. Οπότε η βάση δεδομένων είναι μια βάση ψηφιακών εικόνων.

Σύγκριση προτύπων: Το γενετικό ταίριασμα είναι μια διαδικασία σύγκρισης των δυο ψηφιακών εικόνων μεταξύ τους. Η σύγκριση όμως δεν γίνεται σε πραγματικό χρόνο. Πρέπει να επιβλέπουν επιστήμονες.

Δήλωση ενός ταιριάσματος: Η διαδικασία αυτή γίνεται από επιστήμονες με τη βοήθεια υπολογιστή. Καταρχήν ο αναλυτής πρέπει να κάνει κάποιους εργαστηριακούς ελέγχους έτσι ώστε να διαπιστωθεί αν τα δυο πρότυπα είναι συγκρίσιμα. Στη συνέχεια πρέπει να αποφασίσει αν ταιριάζουν σύμφωνα με κάποιο κριτήριο σύγκρισης.

Εφαρμογές

Το γενετικό αποτύπωμα εκτός από τις ιατρικές εφαρμογές, όπως διάγνωση ανωμαλιών ή κληρονομικών νοσημάτων, χρησιμοποιείται ευρέως για τεστ πατρότητας, αυθεντικοποίηση χρηστών και στην εγκληματολογία. Χρησιμοποιείται επίσης σε μερικές περιπτώσεις για αναγνώριση χρηστών. Στις ΗΠΑ, για παράδειγμα, υπάρχει μια συσκευή που ονομάζεται DNA PAK (Personal Archival Kit) και έχει σα στόχο τη διατήρηση ενός δείγματος γενετικού υλικού έτσι ώστε κάποιο άτομο να μπορεί να αναγνωριστεί σε περιπτώσεις απαγωγών, ατυχημάτων ή φυσικών καταστροφών. Λόγω αυξημένου κόστους παραγωγής και καχυποψίας του κοινού δεν θα δούμε συστήματα αναγνώρισης γενετικού υλικού σε ευρεία κλίμακα.

Σύγκριση τεχνολογιών

Δεν υπάρχει ένα "τέλειο βιομετρικό" το οποίο να καλύπτει όλες τις ανάγκες μας. Κάθε βιομετρικό σύστημα έχει τα πλεονεκτήματα και τα μειονεκτήματά του. Υπάρχουν βέβαια κάποια κοινά χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για σύγκριση.

Βιομετρικό χαρακτηριστικό	Καθολικότητα	Μοναδικότητα	Μονιμότητα	Ικανότητα Συλλογής	Κόστος
DNA	**H**	**H**	**H**	**L**	**H**
Δακτυλικό αποτύπωμα	**M**	**H**	**H**	**M**	**M**
Πρόσωπο	**H**	**L**	**M**	**H**	**L**
Ίριδα	**H**	**H**	**H**	**M**	**M**
Αμφιβληστροειδής	**H**	**H**	**M**	**L**	**H**

Τρόπος πληκτρολόγησης	**L**	**L**	**L**	**M**	**L**
Φωνή	**M**	**L**	**L**	**M**	**M**
Υπογραφή	**L**	**L**	**L**	**H**	**L**

Πίνακας 2. Αξιολόγηση βιομετρικών χαρακτηριστικών

ΚΕΦΑΛΑΙΟ 3: Ο ΑΝΤΙΚΤΥΠΟΣ ΣΤΗΝ ΚΟΙΝΩΝΙΑ

Ασφάλεια (Security)

Τα βιομετρικά συστήματα είναι πιο ασφαλή από τα παραδοσιακά συστήματα αυθεντικοποίησης. Προσφέρουν έναν πολύ ισχυρό δεσμό μεταξύ του φυσικού προσώπου και της ταυτότητάς του. Αυτό σημαίνει ότι η ακεραιότητα της διαδικασίας πρέπει να είναι υψηλή. Η ασφάλεια ενός συστήματος αυθεντικοποίησης χρηστών, δηλαδή ο βαθμός στον οποίο είναι δύσκολο ένας κακόβουλος χρήστης να το παρακάμψει, εξαρτάται από την αρχιτεκτονική ολόκληρού του συστήματος και όχι μόνο από την τεχνολογία που χρησιμοποιείται. Η βιομετρική ασφάλεια δεν μπορεί να στηριχθεί στη μυστικότητα, γιατί υπάρχει ο κίνδυνος αντιγραφής ή κλοπής κάποιων βιομετρικών χαρακτηριστικών. Το πρόσωπο μπορεί εύκολα να φωτογραφηθεί, η φωνή μπορεί να ηχογραφηθεί, το δακτυλικό αποτύπωμα μπορεί να βγει από ένα ποτήρι, ακόμη και το DNA μπορεί να ληφθεί από μια τρίχα. Τα μέτρα που θα λάβουμε λοιπόν, πρέπει να στηρίζονται στα χαρακτηριστικά της διαδικασίας. Όπως αναφέρθηκε προηγουμένως, η βιομετρική αυθεντικοποίηση αποτελείται από τέσσερα στάδια: εγγραφή, αποθήκευση, ανάκτηση και ταίριασμα. Σε κάθε ένα από αυτά τα βήματα υπάρχει πιθανότητα κάποιος κακόβουλος χρήστης να παρεμβληθεί.

Στο στάδιο της εγγραφής, ένας χρήστης εγγράφεται σαν κ. Χ στο σύστημα πριν εγκατασταθεί το βιομετρικό. Αν είναι επιτυχής η εγγραφή με ένα ψεύτικο όνομα, θα είναι αδύνατο να εντοπιστεί η απάτη με το σύστημα αυθεντικοποίησης. Στο επίπεδο της αποθήκευσης, είναι δυνατό να αποκτήσει πρόσβαση στα αποθηκευμένα δεδομένα και να τα παραποιήσει. Όσον αφορά την ανάκτηση, η δυσκολία της κλοπής (spoofing) εξαρτάται από το είδος του βιομετρικού που χρησιμοποιείται. Για παράδειγμα, πιο παλιά με πλαστά δακτυλικά αποτυπώματα μπορούσε πολύ εύκολα ένα σύστημα να παρακαμφθεί. Σήμερα με την εξέλιξη των βιομετρικών συστημάτων

υπάρχουν μηχανισμοί προστασίας, όπως στα αποτυπώματα το τεστ της ζωντάνιας. Όταν ο χρήστης βάζει το χέρι του στον αισθητήρα εκείνος εκπέμπει θερμότητα και ελέγχει τη ροή του αίματος. Ή σε συστήματα αναγνώρισης ίριδας, η δέσμη φωτός που διαπερνά την ίριδα, γίνεται με τέτοιο τρόπο έτσι ώστε να αντιδρά το μάτι και να συστέλλεται ή να διαστέλλεται η κόρη. Ακόμη και στο επίπεδο ταιριάσματος το σύστημα μπορεί να ξεγελαστεί. Αν για παράδειγμα κατά τη διάρκεια του ταιριάσματος, με τη βοήθεια ενός διαχειριστή του συστήματος, μειωθεί το κατώφλι αποδοχής σε τέτοιο σημείο έτσι ώστε η ανίχνευση της εισβολής να μην είναι δυνατή.

Άλλοι παράγοντες που πρέπει να λάβουμε υπόψη μας είναι αν τα δεδομένα είναι κρυπτογραφημένα ή όχι και ο τρόπος μετάδοσης αυτών μεταξύ της κεντρικής βάσης και του συστήματος είναι ασφαλής. Οπότε έχουμε να κάνουμε με πρωτόκολλα επικοινωνίας, ψηφιακές υπογραφές και πιστοποιητικά, πρωτόκολλα SSL, αν η κεντρική μονάδα συνδέεται με πολλά συστήματα αναφερόμαστε σε secured multicast τεχνικές. Τα βιομετρικά σίγουρα είναι ασφαλέστερα από τα παραδοσιακά συστήματα, αλλά δεν είναι τέλεια. Αν αγνοήσουμε την πιθανότητα του λάθους ή της απάτης, η συνολική ασφάλεια του συστήματος μειώνεται, καθώς οι άνθρωποι θα έχουν ακόμη μεγαλύτερη εμπιστοσύνη σε άτομα με ψεύτικη βιομετρική ταυτότητα, από εκείνη που είχαν σε άτομα με ψεύτικη ταυτότητα.

Ιδιωτικότητα (privacy)

Η βιομετρική επαλήθευση και αναγνώριση δημιουργούν ψηφιακά δεδομένα. Δημιουργείται δηλαδή ένα ίχνος που μπορεί να διαβαστεί από τη μηχανή. Από άποψη προστασίας προσωπικών δεδομένων, γεννιούνται ερωτήματα όπως: ποια δεδομένα αποθηκεύονται, πως αποθηκεύονται, ποιος έχει πρόσβαση σε αυτά, για ποιους λόγους τα δεδομένα θα προσπελαστούν; Οι απαντήσεις αυτών των ερωτήσεων και η συμβατότητα με την ισχύουσα νομοθεσία, εξαρτώνται από την αρχιτεκτονική του συστήματος, την πολιτική ασφαλείας της εταιρείας και τα εξειδικευμένα χαρακτηριστικά της εκάστοτε βιομετρικής τεχνικής. Η ιδιωτικότητα συνδέεται πολύ στενά με την αποδοχή από τους χρήστες. Ένα σύστημα αυθεντικοποίησης όπου οι χρήστες του αισθάνονται ότι τα δεδομένα τους δεν προστατεύονται επαρκώς και δεν υπάρχει σεβασμός απέναντι στην ιδιωτικότητά τους, δεν θα έχει ποτέ την απαραίτητη συνεργασία και υποστήριξη για να επιτύχει.

Διαλειτουργικότητα (Interoperability)

Για κάθε νέα τεχνολογία, η διαλειτουργικότητα σε πολλούς επαγγελματικούς τομείς, σε συσκευές και συστήματα, είναι ευεργετική για τη διάχυσή της. Για παράδειγμα, όσο πιο πολλά μηχανήματα μπορούν να διαβάσουν μια μονάδα αποθήκευσης βιομετρικών δεδομένων, τόσο πιο χρήσιμη γίνεται η μονάδα. Αυτό έχει εφαρμογές τόσο σε γεωγραφικό επίπεδο, όπου είναι πολύ χρήσιμο ένα βιομετρικό διαβατήριο να είναι αναγνώσιμο σε πολλά σημεία του πλανήτη, όσο και σε θέματα ενοποίησης τεχνολογιών, όπου μια smart card θα μπορούσε να χρησιμεύει για πρόσβαση σε κάποιο χώρο και ταυτόχρονα να μπορεί κάποιος να κάνει ανάληψη από ένα ATM. Γίνονται προσπάθειες για τη δημιουργία προτύπων (standards) για την προώθηση εφαρμογών ανοικτών συστημάτων. Πρότυπο είναι ένα έγγραφο, το οποίο έχει δημιουργηθεί και εγκριθεί από ένα αναγνωρισμένο οργανισμό και παρέχει κανόνες και κατευθύνσεις για διάφορες δραστηριότητες. Κάποια από τα πρότυπα που χρησιμοποιούνται στα βιομετρικά συστήματα είναι: API - INCITS 358-2002, BioAPI Specification version 1.1. Από το 2000, το NIST (National Institute of Standards and Technology) και η NSA (National Security Agency) συγχρηματοδότησαν και διέδωσαν μια σειρά από δραστηριότητες που σχετίζονται με τα βιομετρικά, με την πιο σημαντική τη δημιουργία του Common Biometric Exchange File Format (CBEFF) (Common Biometric Exchange File Format (CBEFF). Το CBEFF περιγράφει ένα σύνολο δεδομένων αναγκαίο για την υποστήριξη βιομετρικών τεχνολογιών με ένα κοινό τρόπο, ανεξάρτητα από την εφαρμογή ή την πλατφόρμα χρήσης (πχ. υπολογιστής, κινητό). Διευκολύνει την ανταλλαγή βιομετρικών δεδομένων μεταξύ διαφορετικών εξαρτημάτων των συστημάτων ή μεταξύ διαφορετικών συστημάτων, προωθεί τη διαλειτουργικότητα βιομετρικών εφαρμογών, προσφέρει προς τα μπροστά συμβατότητα για τεχνολογικές βελτιώσεις και απλοποιεί τη διαδικασία ολοκλήρωσης του λογισμικό και του hardware.

Όμως, σε αντίθεση με τις υπόλοιπες τεχνολογίες, η διαλειτουργικότητα στα βιομετρικά δε είναι πάντα επιθυμητή. Αυτό γιατί η απουσία καθολικής διαλειτουργικότητας μπορεί να δημιουργήσει φραγμούς στην μεταφορά και εκμετάλλευση προσωπικών δεδομένων. Όμως αφού η τεχνολογική διαλειτουργικότητα είναι κάτι που δύσκολα θα αποφευχθεί, πρέπει να βρεθούν άλλοι τρόποι προστασίας.

Αφού οι χρήστες έχουν στη διάθεσή τους πολλά βιομετρικά, πιθανότατα διαφορετικές εφαρμογές θα χρησιμοποιούν διαφορετικά βιομετρικά. Επίσης συστήματα που δεν είναι βιομετρικά συμβατά, για παράδειγμα ένας αναγνώστης δακτυλικών αποτυπωμάτων και ένας αναγνώστης ίριδας, μπορούν να επικοινωνήσουν σε επίπεδο δεδομένων και να ανταλλάσουν δεδομένα έτσι ώστε να διαπιστωθεί ο χρόνος και ο τόπος που έγινε μια αυθεντικοποίηση χρήστη.

Το μεγαλύτερο θέμα που θα πρέπει να μας απασχολεί είναι οι διεθνείς περιπτώσεις στις οποίες συναντάμε τα βιομετρικά. Για παράδειγμα στον έλεγχο των συνόρων. Αν μια βιομετρική επαλήθευση ταυτότητας επιστρέψει αρνητικό αποτέλεσμα, θα πρέπει το αποτέλεσμα αυτό να ερμηνεύεται με τον ίδιο τρόπο σε όλο τον κόσμο.

Οικονομικές πλευρές – Κόστος (Cost)

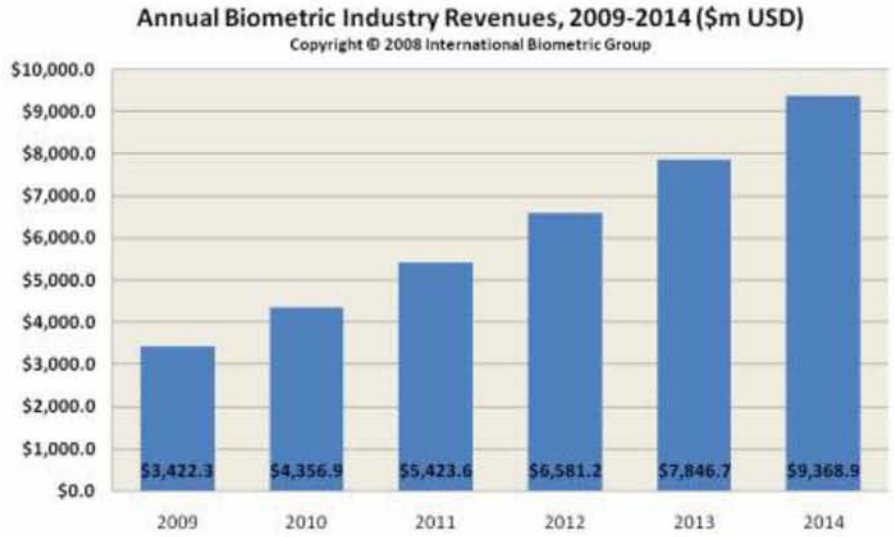
Αν υποθέσουμε ότι η "φοβία" μιας νέας τεχνολογίας μπορεί να ξεπεραστεί, τότε ο μεγαλύτερος ανασταλτικός παράγοντας υιοθέτησης των βιομετρικών τεχνολογιών είναι το κόστος.

Όπως κάθε σύστημα αυθεντικοποίησης, έτσι και τα συστήματα βιομετρικής αυθεντικοποίησης έχουν κάποιο κόστος. Το κόστος αυτό ποικίλλει από τεχνολογία σε τεχνολογία. Για παράδειγμα ένα σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων, κοστίζει πολύ περισσότερο από ένα σύστημα αναγνώρισης πληκτρολόγησης κειμένου. Μια συσκευή αναγνώρισης δακτυλικών αποτυπωμάτων κοστίζει 450$, ενώ μια συσκευή αναγνώρισης πληκτρολόγησης κοστίζει 210$. Αλλά ακόμη και στην ίδια τεχνολογία υπάρχουν μεγάλες διαφορές, μεταξύ εξοπλισμού που χρησιμοποιεί τις τελευταίες εξελίξεις της τεχνολογίας και ενός συστήματος που χρησιμοποιεί πιο παλιά χαρακτηριστικά. Πρέπει επίσης να λάβουμε υπόψη το μέγεθος της υλοποίησης, γιατί τα σταθερά κόστη μπορεί να εξαπλωθούν σε μια μεγάλης κλίμακας εφαρμογή. Ο υπολογισμός του κόστους περιέχει επίσης μέτρα που θα διασφαλίσουν την ασφάλεια των δεδομένων (κρυπτογράφηση, firewall, SSL). Τέλος, είναι σημαντικό να συμπεριλάβουμε και τα κόστη του βοηθητικού συστήματος και της εγκατάστασης και καλής λειτουργίας της διαδικασίας της εγγραφής.

Τα βιομετρικά συστήματα είναι συστήματα πολύ ισχυρής αυθεντικοποίησης, συνεπώς επηρεάζουν το επίπεδο "εμπιστοσύνης" στις οικονομικές συναλλαγές. Με άλλα λόγια μπορούν να βοηθήσουν στη μείωση της απάτης και να απολαύσει ο

καθένας τα οφέλη της Κοινωνίας της Πληροφορίας. Απλοποιώντας τα πράγματα από την πλευρά του χρήστη περιορίζεται το λάθος στο ελάχιστο. Συγχρόνως, η διαδεδομένη χρήση τους θα βοηθήσει τους καταναλωτές να νιώσουν μεγαλύτερη ασφάλεια και ίσως να μειωθεί το κόστος ανά ασφαλή συναλλαγή.

Αυτός είναι και ο λόγος που ο Διεθνής Οργανισμός Βιομετρικών (International Biometric Group) αναμένει ότι η αγορά των βιομετρικών σχεδόν θα τριπλασιαστεί μέχρι το 2014 (Biometric Market and Industry Report 2009-2014). Η συγκεκριμένη αναφορά έχει κάποια πολύ ενδιαφέροντα στοιχεία. Πιο συγκεκριμένα, αναφέρει ότι η αγορά των βιομετρικών από 3,42 δις $ το 2009 θα αυξηθεί στα 9,37 δις $ το 2014, και σε αυτό θα συμβάλει η διαχείριση ταυτοτήτων από την κυβέρνηση και τα προγράμματα διαχείρισης και ελέγχου συνόρων. Η αναγνώριση δακτυλικών αποτυπωμάτων αναμένεται να καλύψει το 45,9% της αγοράς, ακολουθούμενη από την αναγνώριση προσώπου σε ποσοστό 18,5% και της αναγνώρισης ίριδας σε ποσοστό 8,3%. Η Ασία και η Βόρεια Αμερική αναμένεται να είναι οι μεγαλύτερες αγορές για βιομετρικά προϊόντα και υπηρεσίες.



Γράφημα 3. Αγορά Βιομετρικών 2009-2014

Το χαμηλό κόστος είναι σημαντικό, αλλά οι περισσότεροι κατασκευαστές κατανοούν ότι δεν είναι μόνο το αρχικό κόστος ενός σένσορα, του λογισμικού εγγραφής, συντήρησης των προτύπων (template aging) και το αναγκαίο ανθρώπινο δυναμικό. Συχνά, το κόστος παροχής διαχείρισης και σωστής λειτουργίας του συστήματος μπορεί να ξεπεράσει το αρχικό κόστος του βιομετρικού εξοπλισμού. Θα πρέπει όμως να έχουμε υπόψη μας ότι και τα προηγούμενα συστήματα έχουν "κρυφά" κόστη,

όπως για παράδειγμα εφαρμογές υπενθύμισης passwords, αντικατάσταση εγγράφων, κόστη από λάθη.

Θέματα διαλειτουργικότητας και πρότυπα (standards) όμως, καθορίζουν την ευρεία αποδοχή και διαμορφώνουν οικονομικές προκλήσεις.

Τα ακόλουθα αντικείμενα συνοψίζουν τις οικονομικές συνέπειες των βιομετρικών:

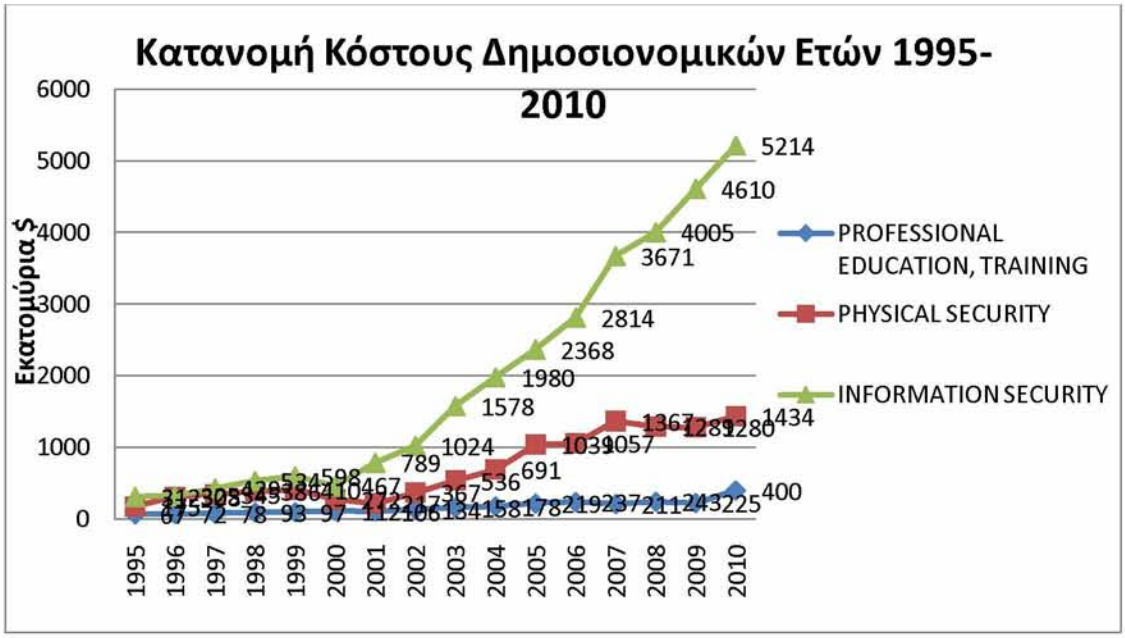
1. Η έννοια της βέλτιστης ταυτότητας. Η οικονομική σημασία της ταυτότητας, αυξάνεται σε μια ψηφιακή κοινωνία, αλλά η πιο ισχυρή προστασία της δεν είναι απαραίτητα και η καλύτερη.
2. Αρνητικές συνέπειες της ισχυρής αυθεντικοποίησης. Λάθη στην αυθεντικοποίηση μπορεί να μη συμβαίνουν τόσο συχνά, αλλά όταν συμβούν, ενδεχομένως θα είναι και πιο επικίνδυνα. Για παράδειγμα, η κλοπή ταυτότητας μπορεί να είναι πιο σπάνια, αλλά αν γίνει θα είναι πιο σοβαρή και με ευρύτερες κοινωνικές επιπτώσεις.
3. Η διαλειτουργικότητα είναι ζωτικής σημασίας για τη λειτουργία της αγοράς. Υπάρχει σοβαρός κίνδυνος η αγορά βιομετρικών και οι αγορές που εξαρτώνται από την αυθεντικοποίηση, μπορεί να κατακερματιστούν σε clusters, οι οποίες δε θα αλληλοσυνεργάζονται, έτσι γίνονται τρωτές στα μονοπώλια ή στην κυριαρχία λίγων παιχτών.
4. Εμπλοκή πνευματικών δικαιωμάτων στην ανάπτυξη βιομετρικών συστημάτων απειλούν τον ανταγωνισμό. Η ανεξέλεγκτη εκμετάλλευση των πνευματικών δικαιωμάτων των τεχνολογιών βιομετρίας, μπορεί να, μειώσει τον ανταγωνισμό και να διαταράξει την ανάπτυξη, καθώς και την κατανόησή τους.
5. Η κατανόησή τους και κατ' επέκταση η χρησιμοποίηση στο δημόσιο τομέα, θα διαμορφώσει την αγορά. Η χρήση των βιομετρικών στην ηλεκτρονική διακυβέρνηση και σε μεγάλης κλίμακας δημόσιες συνδιαλλαγές, θα αποτελέσει σημείο κλειδί για την εξασφάλιση ανοιχτών και ανταγωνιστικών αγορών.

Στον Πρόεδρο των Η.Π.Α. κάθε χρόνο παραδίδεται μια αναφορά από το Security Oversite Office (ISOO), για τα εκτιμώμενα κόστη διαβάθμισης ασφαλείας ενός δημοσιονομικού έτους. Για το έτος 2010 έχουμε το παρακάτω γράφημα στο οποίο φαίνεται ότι το συνολικό κόστος ανέρχεται στα 7 δις $. Τα στοιχεία αυτά έρχονται

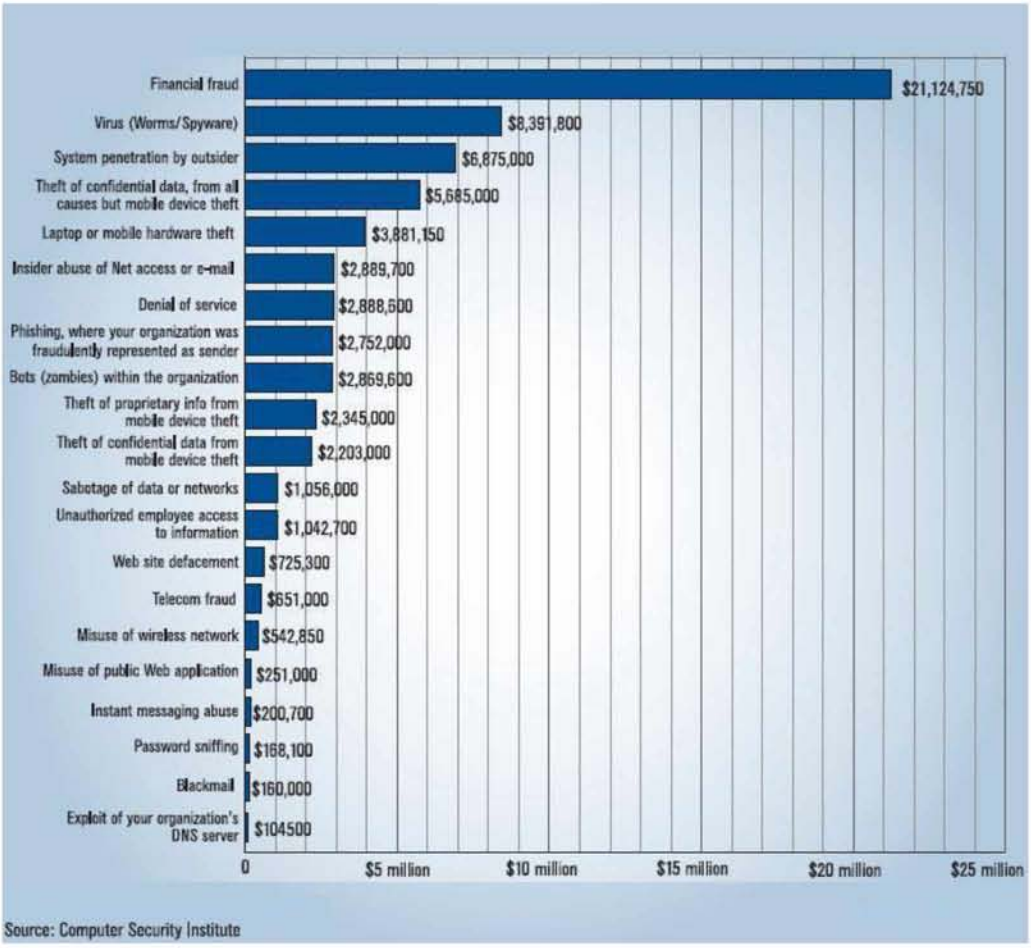
από 41 διαφορετικές υπηρεσίες, όπως το Υπουργείο Άμυνας και τη CIA. (2010 cost report)

Γράφημα 4.

Στο παρακάτω γράφημα έχουμε μια συγκεντρωτική αναφορά από το 1995 έως το 2010 και μπορούμε να παρατηρήσουμε τη ραγδαία αύξηση κυρίως του κόστους για την ασφάλεια πληροφοριών.



Γράφημα 5.



Γράφημα 6. Απώλειες σε εκατομμύρια δολάρια από διάφορα είδη απειλών το 2009

Νομικά ζητήματα (Legal)

Μέχρι τώρα η βιομετρική τεχνολογία λειτουργούσε σε αρκετά κλειστά περιβάλλοντα. Το υπάρχον νομικό πλαίσιο δεν παρεμποδίζει δημόσιες και ιδιωτικές πρωτοβουλίες από το να αναπτυχθούν τέτοιου είδους εφαρμογές. Η ανάπτυξη των βιομετρικών δεν απειλεί διαδικαστικά δικαιώματα, όπως δικαιώματα στο δικαστήριο. Αν και το γεγονός ότι έχουν δημιουργηθεί κάποια ζητήματα εξαιτίας του νομικού πλαισίου που ισχύει για την προστασία δεδομένων, αυτό δεν αποτέλεσε εμπόδιο για τις πρόσφατες επιλογές για τα βιομετρικά στα ευρωπαϊκά διαβατήρια. Όμως η ευρεία εφαρμογή τους και ο φόβος μιας κοινωνίας "επιτήρησης" εξαιτίας του "φαινομένου της διάχυσης", επιβάλλουν την αναθεώρηση των διαθέσιμων νομικών εργαλείων. Αν εξαιρέσουμε την ανάλυση DNA, την αναγνώριση δακτυλικών αποτυπωμάτων και την αναγνώριση προσώπου, δεν υπάρχει αρκετή νομοθεσία στην Ευρώπη που να αφορά τα βιομετρικά. Τα βιομετρικά που χρησιμοποιούνται σε ιδιωτικές συνδιαλλαγές βασίζονται στη συγκατάβαση. Όταν όμως η χρήση τους γίνεται υποχρεωτική, όπως

για παράδειγμα στα ηλεκτρονικά διαβατήρια, θα χρειαστεί καινούρια νομοθεσία. Πολύ σημαντική είναι η ιδιωτικότητα, ένα θεμελιώδες δικαίωμα όπως αναφέρεται στο άρθρο 8 της Ευρωπαϊκής Συνθήκης για την Προστασία των Ανθρώπινων Δικαιωμάτων και θεμελιωδών ελευθεριών. Ανάμειξη στα δικαιώματα και στις ελευθερίες του ατόμου θα πρέπει να απαγορεύεται ρητά, εκτός και αν συντρέχει νόμιμος λόγος για να γίνει κάτι τέτοιο.

Τα περισσότερα βιομετρικά δεν απαιτούν διείσδυση στο ανθρώπινο σώμα, οπότε μπορεί να υποτεθεί ότι η χρήση αυτών των τεχνολογιών δεν θα θεωρηθεί αδικαιολόγητα παρεμβατική όταν βασίζεται στο νόμο ή τη συγκατάθεση. Οπότε κάθε εφαρμογή , όπως η χρησιμοποίηση βιομετρικών στα διαβατήρια και στο σύστημα της Visa από τον Ευρωπαίο νομοθέτη, θα πρέπει να εκπληρώνει τέσσερις προϋποθέσεις: αξιοπιστία, αναλογικότητα, την ύπαρξη επιλογής υποχώρησης και τη συγκατάθεση ή την εξ' αρχής γνώση. Ακόμα κι αν υπάρξουν διαφωνίες με την τωρινή ευρωπαϊκή νομοθεσία, όταν αυτές οι τέσσερις προϋποθέσεις εκπληρώνονται, οι αποφάσεις τηρούν την Ευρωπαϊκή Συνθήκη των Ανθρωπίνων Δικαιωμάτων.

Πρωταρχικά, θα πρέπει να αποφασιστεί το κατά πόσο τα βιομετρικά θα επιτρέπονται και πότε. Η ανάπτυξη εννοιών όπως "βιομετρική ανωνυμία" και "δικαίωμα ιδιοκτησίας βιομετρικών δεδομένων", ίσως βοηθήσει στην επίτευξη αυτού του στόχου. Μόλις ο νομοθέτης καθορίσει τη νόμιμη χρήση τους, έπεται ενίσχυση των διαθέσιμων εργαλείων διαφάνειας. Μόνο μετά την αναγνώριση της νόμιμης χρήσης των βιομετρικών διαδικασιών, θα πρέπει να καθοριστούν κανόνες και συνθήκες ορθής χρήσης. Συνεπώς υπάρχει ανάγκη βασικών αρχών, όπως: ισότητα πρόσβασης στο δίκτυο, απόλυτη ακρίβεια στόχευσης από κλειστά συστήματα παρακολούθησης, συστήματα που θα εξασφαλίζουν την ακρίβεια των δεδομένων που διατηρούνται από τέτοια συστήματα, μηχανισμούς τροποποίησης ψεύδους, μη ακριβή ή τροποποιημένα δεδομένα, συστήματα για να προστατευθούν οι χρήστης από την κλίση τους να ανταλλάσουν την ιδιωτικότητά τους. Αυτό το βιομετρικό πλαίσιο θα πρέπει να είναι βασισμένο σε κατάλληλη ανάλυση επικινδυνότητας (risk assessment), το οποίο διακρίνει τη νόμιμη από τη μη νόμιμη χρήση των βιομετρικών.

Από τη στιγμή που η ανάλυση DNA προσφέρει πολύ μεγαλύτερη ασφάλεια και αξιοπιστία από παλαιότερες μεθόδους συλλογής αποδεικτικών στοιχείων, υπάρχει ο κίνδυνος ότι οι δικαστές θα μπουν στη διαδικασία να παραχωρήσουν πολύ σημαντικό ρόλο στη λήψη αποφάσεων στη συγκεκριμένη βιομετρική τεχνική (με την προϋπόθεση ότι η διαδικασία γίνεται σωστά και από πιστοποιημένους οργανισμούς).

Αυτό μπορεί να είναι επιζήμιο στο σύστημα της ελεύθερης αξιολόγησης των αποδείξεων από τους δικαστές. Αυτή η προειδοποίηση μπορεί να γενικευτεί σε όλες τις βιομετρικές τεχνικές και σε όλα τα συστήματα συλλογής αποδείξεων στην Ευρώπη. Όποτε οι έρευνες γίνονται πολύπλοκες και οι μέθοδοι της έρευνας γίνονται επίσημες, το αποτέλεσμα θα γίνεται όλο και πιο δύσκολο να αξιολογηθεί από το δικαστήριο και την υπεράσπιση. Για να αποτρέψουμε τους ειδικούς να πάρουν τη θέση των δικαστών, χρειάζεται νόμιμη αναγνώριση του δικαιώματος της αντεξέτασης.

Ελληνική πραγματικότητα

Όσον αφορά την Ελλάδα, αρμόδιο όργανο για θέματα που αφορούν τα βιομετρικά είναι η Αρχή Προστασίας Δεδομένων. Παρακάτω παραθέτονται κάποια παραδείγματα αποφάσεων της Αρχής που έχουν να κάνουν με απαγόρευση ή μη της χρήσης βιομετρικών τεχνολογιών.

Ελληνική Δημοκρατία. Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα

31/03/2003 Α.Π. 384

Η Αττικό Μετρό ΑΕ (συντ.ΑΜΕΛ)στις 29-8-2002 με έγγραφό της (α.π. 1834/29-8-2002) απεύθυνε ερώτημα προς την Αρχή Προστασίας Δεδομένων για τη νομιμότητα εφαρμογής, σύμφωνα με τις διατάξεις του Ν.2472/1997 και την Οδηγία 115/2001 της Αρχής, αναλυτών βιομετρικής τεχνολογίας σε εγκαταστάσεις υψηλού κινδύνου του Μετρό. Η ΑΜΕΛ στο παραπάνω έγγραφο διατυπώνει την άποψη ότι ο έλεγχος πρόσβασης στις «κρίσιμες» εγκαταστάσεις του Μετρό, πρέπει να εφαρμόζεται με τα πιο αποτελεσματικά τεχνικά και οργανωτικά μέσα για την επίτευξη της μέγιστης ασφάλειας επιτήρησης των συγκεκριμένων χώρων. Για τον σκοπό αυτό προτείνει την εγκατάσταση συσκευών ελέγχου πρόσβασης βιομετρικής τεχνολογίας.

Πιλοτική εφαρμογή του προτεινόμενου συστήματος εξετάστηκε με επιτόπιο έλεγχο στις 5-9-2002, από τις ελέγκτριες κ.Σιουγλέ και κ.Καμπουράκη ενώ παράλληλα ζητήθηκαν και εγγράφως επιπλέον πληροφορίες για τον τρόπο λειτουργίας του. Από τον έλεγχο διαπιστώθηκαν τα εξής: α)το σύστημα καταγράφει αποκλειστικά με ψηφιακό τρόπο στοιχεία της γεωμετρίας του χεριού του χρήστη. Δεν συλλέγει άλλα στοιχεία όπως είναι για παράδειγμα τα δακτυλικά αποτυπώματα. β) Το σύστημα θα χρησιμοποιηθεί αποκλειστικά για τον σκοπό του ελέγχου πρόσβασης των εργαζομένων σε κρίσιμες εγκαταστάσεις των σταθμών του Μετρό. γ)Αποτελείται από συσκευές οι οποίες είναι αυτόνομες και δεν υπάρχει διασύνδεση στοιχείων με

κεντρική βάση δεδομένων. Στις συσκευές επίσης δεν καταγράφονται άλλα προσωπικά στοιχεία όπως για παράδειγμα το ονοματεπώνυμο του χρήστη.

Το παραπάνω θέμα εξετάστηκε το Νοέμβριο του 2002 από το Συμβούλιο της Αρχής και αποφασίστηκε ότι η εγκατάσταση του παραπάνω συστήματος αποτελεί ένα ανάλογο μέτρο προστασίας σύμφωνα με το άρθρο 10 του Ν.2472/1997. Όπως ειδικά αναφέρει η Οδηγία αρ.115/2001της Αρχής για τα θέματα επεξεργασίας προσωπικών δεδομένων εργαζομένων, η χρήση βιομετρικών μεθόδων είναι επιτρεπτή μόνο σε περιπτώσεις που αυτό επιβάλλεται από ιδιαίτερες απαιτήσεις ασφάλειας των χώρων εργασίας και εφόσον δεν υπάρχει άλλο μέσο για την επίτευξη του σκοπού αυτού. Λαμβάνοντας υπόψη ότι ο σκοπός εφαρμογής του παραπάνω συστήματος της ΑΜΕΛ είναι αποκλειστικά ο έλεγχος της πρόσβασης στους συγκεκριμένους χώρους για την αποφυγή μη εξουσιοδοτημένης εισόδου από τρίτους, η ΑΜΕΛ οφείλει να σταθμίσει τους υπάρχοντες κινδύνους, την έκταση των κινδύνων αυτών και τις υπάρχουσες εναλλακτικές δυνατότητες αντιμετώπισης των κινδύνων, και αφετέρου, την πιθανότητα παραβίασης της ιδιωτικότητας των εργαζομένων από την εφαρμογή της βιομετρικής τεχνολογίας.

Η Αρχή στις 26-11-2002 απέστειλε σχετικό έγγραφο στην ΑΜΕΛ στο οποίο ανέφερε τα παραπάνω, ότι δηλαδή η ΑΜΕΛ προτού προβεί σε ενέργειες εγκατάστασης ενός βιομετρικού συστήματος, οφείλει προηγουμένως να εκπονήσει ανάλυση επικινδυνότητας του πληροφοριακού συστήματός της, η οποία καταλήγει σε συγκεκριμένα τεχνικά και οργανωτικά μέτρα προστασίας. Η στάθμιση παραγόντων «απειλή» – «ευπάθεια» – «ενδεχόμενη ζημιά» ορίζει το πλαίσιο επιλογής των ανάλογων μέτρων προστασίας.

Η ΑΜΕΛ με έγγραφό της στις 26-2-2003 ενημέρωσε την Αρχή ότι ολοκλήρωσε τη μελέτη επικινδυνότητας του πληροφοριακού συστήματος του Μετρό (αντίγραφο της οποίας κοινοποιήθηκε στην Αρχή) σύμφωνα με τις συστάσεις της τελευταίας. Στις λειτουργικές συστάσεις της παραπάνω μελέτης προτείνεται η αξιοποίηση «ήπιων» βιομετρικών τεχνολογιών (βασισμένων σε χαρακτηριστικά που δεν αφήνουν ίχνη). Ο αποκλειστικός σκοπός εφαρμογής τους είναι ο έλεγχος πρόσβασης σε εγκαταστάσεις υψηλής επικινδυνότητας της ΑΜΕΛ. Υποστηρίζεται η άποψη ότι δεν πρέπει να τηρούνται τα σχετικά δεδομένα σε κεντρική βάση δεδομένων ενώ λαμβάνεται υπόψη και η αρχή της τήρησης των ελάχιστων προσωπικών δεδομένων για την εκπλήρωση του συγκεκριμένου σκοπού. Επίσης στις λειτουργικές συστάσεις της ίδιας μελέτης αναφέρονται ρητά οι συγκεκριμένοι χώροι

στους οποίους συστήνεται, ως σκόπιμη και αναγκαία για την επαρκή ασφάλειά τους, η χρήση βιομετρικών συσκευών για τον έλεγχο της πρόσβασης.

Μετά από εξέταση όλων των παραπάνω στοιχείων και κατόπιν διαλογικής συζήτησης

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

Το άρθρο 2 του Νόμου 2472/1997, ορίζει ότι «δεδομένα προσωπικού χαρακτήρα» είναι κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. «Υποκείμενο των δεδομένων» είναι, το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική. Σύμφωνα με τον παραπάνω ορισμό τα δεδομένα που χρησιμοποιούνται για την ταυτοποίηση ενός προσώπου με χρήση βιομετρικών μεθόδων ή αλλιώς, η ψηφιακή απεικόνιση ενός φυσικού χαρακτηριστικού, αποτελούν προσωπικά δεδομένα.

Σύμφωνα με το άρθρο 4 της Νόμου 2472/1997, τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών. Επίσης τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.

Η παραπάνω αρχή του σκοπού προϋποθέτει τον σαφή ορισμό του σκοπού για τον οποίο θα γίνει συλλογή και επεξεργασία βιομετρικών δεδομένων. Η αξιολόγηση των ζητημάτων της αναλογικότητας και νομιμότητας εφαρμογής του σκοπού είναι απαραίτητη, λαμβάνοντας υπόψη τους κινδύνους που θέτει η χρήση των βιομετρικών τεχνολογιών σχετικά με την προστασία των πρωταρχικών δικαιωμάτων και ελευθεριών του ατόμου.

Στην Οδηγία 112/2001 ως νόμιμος σκοπός για την επεξεργασία βιομετρικών δεδομένων ορίζεται αυτός που αφορά την εφαρμογή ιδιαίτερων απαιτήσεων ασφάλειας των χώρων εργασίας λαμβάνοντας υπόψη ότι δεν υπάρχει άλλο μέσο για την επίτευξη του σκοπού αυτού. Ο υπεύθυνος της επεξεργασίας οφείλει με τρόπο συστηματικό, να σταθμίζει από τη μια πλευρά την αναγκαιότητα εφαρμογής των βιομετρικών τεχνολογιών και από την άλλη τα δικαιώματα των εργαζομένων.

Σύμφωνα με το Ν.2472/1997, δεν επιτρέπεται η επεξεργασία δεδομένων για άλλο σκοπό από εκείνον που εξαρχής συλλέχθηκαν. Επομένως η παραπάνω συλλογή

βιομετρικών στοιχείων είναι επιτρεπτή αποκλειστικά για τον σκοπό του ελέγχου πρόσβασης. Η χρήση τους για άλλο σκοπό όπως για παράδειγμα για την αξιολόγηση συμπεριφοράς του εργαζομένου είναι ασυμβίβαστη με τον πρωταρχικό σκοπό και δεν επιτρέπεται.

Για τον σκοπό του ελέγχου πρόσβασης το προτεινόμενο βιομετρικό σύστημα, σύμφωνα με τις λειτουργικές συστάσεις της ανάλυσης επικινδυνότητας, σχετίζεται με φυσικά χαρακτηριστικά που δεν αφήνουν ίχνη (πχ γεωμετρία χεριού αλλά όχι δακτυλικά αποτυπώματα) και επομένως ελαχιστοποιούνται οι κίνδυνοι για την παραβίαση των δικαιωμάτων του ατόμου.

Η ΑΜΕΛ σύμφωνα με το άρθρο 10 του Ν.2472/1997 οφείλει να λαμβάνει όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα ασφάλειας για την προστασία των προσωπικών δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Μέτρα ασφάλειας επομένως πρέπει να εφαρμοστούν κατά την επεξεργασία των βιομετρικών δεδομένων (αποθήκευση, μετάδοση, εξαγωγή χαρακτηριστικών και σύγκριση κλπ.).

Για τους λόγους αυτούς:

Η Αρχή Προστασίας Δεδομένων κρίνει ότι η εγκατάσταση βιομετρικού συστήματος αποκλειστικά για τον σκοπό του ελέγχου της πρόσβασης των εργαζομένων στις κρίσιμες εγκαταστάσεις της εταιρείας «Αττικό Μετρό ΑΕ» δεν παραβιάζει τα δικαιώματα των εργαζομένων της σύμφωνα με όσα ορίζονται στην Οδηγία 115/2001 της Αρχής, εφόσον πληρούνται οι λειτουργικές συστάσεις της μελέτης επικινδυνότητας της Αττικό Μετρό. Συγκεκριμένα πρέπει οι συσκευές βιομετρικής τεχνολογίας που θα εγκατασταθούν να χαρακτηρίζονται «ήπιες» όπως αναφέρεται στο ιστορικό της απόφασης αυτής και να έχουν τα εξής χαρακτηριστικά: να μην τηρούνται τα προσωπικά δεδομένα των εργαζομένων σε κεντρική βάση δεδομένων, η επεξεργασία να εκτελείται αποκλειστικά για τον σκοπό του ελέγχου πρόσβασης των εργαζομένων της ΑΜΕΛ σε κρίσιμες εγκαταστάσεις, να τηρούνται τα ελάχιστα για την εκπλήρωση του συγκεκριμένου σκοπού προσωπικά δεδομένα και μόνο για το χρονικό διάστημα που είναι αναγκαίο για την εκτέλεση της επεξεργασίας. Επομένως η παραπάνω επεξεργασία κρίνεται νόμιμη με την προϋπόθεση ότι τηρούνται οι όροι και οι προϋποθέσεις που προαναφέρθηκαν.

Ο υπεύθυνος της επεξεργασίας οφείλει σύμφωνα με το άρθρο 11 του Ν.2472/1997 να ενημερώσει τους εργαζομένους για την εφαρμογή του παραπάνω

συστήματος. Η ενημέρωση πρέπει να περιλαμβάνει τουλάχιστον τον ακριβή ορισμό του σκοπού που επιβάλλει τη χρήση του βιομετρικού συστήματος, καθώς και τον τόπο και χρόνο της επεξεργασίας.

Ελληνική Δημοκρατία. Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα
23/06/2004 Α.Π. 1450

Ο Διεθνής Αερολιμένας Αθηνών «ΕΛ. ΒΕΝΙΖΕΛΟΣ» (ΔΑΑ) μας γνωστοποίησε με το έγγραφό του ότι διερευνά νέες μεθόδους για την περαιτέρω ενίσχυση του υπάρχοντος συστήματος ελέγχου πρόσβασης –προσπέλασης, με σκοπό την καλύτερη δυνατή διασφάλιση της πρόσβασης στο Κέντρο Επιχειρήσεων του Αερολιμένα (ΚΕΑ) – Airport Services Operations Center (ASOC). Στο πλαίσιο αυτό, ο Διεθνής Αερολιμένας Αθηνών έχει την πρόθεση να εφαρμόσει πιλοτικά βιομετρική τεχνολογία. Το προτεινόμενο σύστημα επαλήθευσης της ταυτότητας βασίζεται στα βιομετρικά χαρακτηριστικά της ίριδας και των δύο οφθαλμών. Προϋποθέτει δε μια φάση προετοιμασίας ή εγγραφής, κατά την οποία οι υπάλληλοι που έχουν δικαίωμα πρόσβασης στο ΚΕΑ θα προσέρχονται στο γραφείο έκδοσης αδειών εισόδου του Αερολιμένα και θα υποβάλλονται στην ανάγνωση από κατάλληλες συσκευές των βιομετρικών τους χαρακτηριστικών. Τα βιομετρικά τους στοιχεία θα αποθηκεύονται κρυπτογραφημένα σε ‘έξυπνες κάρτες’ (smart cards), μαζί με το ονοματεπώνυμό τους, την εταιρία στην οποία εργάζονται, ημερομηνία λήξης της κάρτας (αν υπάρχει), καθώς και μοναδικό κωδικό αριθμό της κάρτας, ο οποίος δίνεται στο πλαίσιο του συστήματος ελέγχου πρόσβασης του Αερολιμένα. Βιομετρικά χαρακτηριστικά υπαλλήλων θα αποθηκεύονται μόνο στις smart cards και όχι σε συγκεντρωτική βάση της εταιρίας. Κάθε φορά που ένας υπάλληλος θα ελέγχεται προκειμένου να εισέλθει στο ΚΕΑ, αυτός θα παρουσιάζει την ‘έξυπνη κάρτα’ του και ταυτόχρονα θα υποβάλλεται σε ιριδοσκόπηση και των δύο οφθαλμών. Τα βιομετρικά στοιχεία τα οποία θα σχηματίζονται από την τρέχουσα ανάγνωση της ίριδος των ματιών θα συγκρίνονται με αυτά που είναι αποθηκευμένα στην έξυπνη κάρτα και, εφόσον ταυτίζονται, θα επιτρέπεται η είσοδος στο ΚΕΑ. Διαφορετικά, δεν θα επιτρέπεται η είσοδος στο ΚΕΑ. η Αρχή με απόφασή της 5-11-2003 (α.α. 52/2003), έκρινε ως μη νόμιμη τη συλλογή και επεξεργασία δεδομένων δακτυλοσκόπησης και ίριδας του οφθαλμού στο Διεθνή Αερολιμένα Αθηνών, στα πλαίσια του πιλοτικού προγράμματος S-Travel, για την επαλήθευση της ταυτότητας των επιβατών που πρόκειται να ταξιδέψουν, επειδή, εξεταζόμενη υπό το πρίσμα των αρχών του σκοπού

και της αναγκαιότητας, υπερβαίνει την επεξεργασία προσωπικών δεδομένων που είναι αναγκαία για την επίτευξη του επιδιωκόμενου από το εν λόγω πιλοτικό πρόγραμμα σκοπού. β) Αντιθέτως, με την απόφαση της 31-03-2003 (α.α. 9/2003) η Αρχή, αφού επανέλαβε όσα αναφέρονται στην προηγούμενη απόφασή της, έκρινε, εφαρμόζοντας τα ίδια κριτήρια, ότι δεν παραβιάζονται τα, σύμφωνα με την οδηγία 115/2001 της Αρχής, δικαιώματα των εργαζομένων με την εγκατάσταση βιομετρικού συστήματος (στοιχεία της γεωμετρίας του χεριού) αποκλειστικώς για τον σκοπό του ελέγχου πρόσβασής τους στις κρίσιμες (ενν. ιδιαίτερα ευαίσθητες από πλευράς ασφαλείας των συγκοινωνιών) εγκαταστάσεις του Αττικού Μετρό. Όπως από τις αποφάσεις αυτές συνάγεται, κάθε σχετικό ζήτημα πρέπει να κρίνεται αυτοτελώς βάσει των πραγματικών στοιχείων που το συνοδεύουν.

Στη συγκεκριμένη περίπτωση, το Κέντρο Επιχειρήσεων του Αερολιμένα περιγράφεται από το Διεθνή Αερολιμένα Αθηνών και αναγνωρίζεται ως χώρος νευραλγικής σημασίας και υψίστης ασφαλείας και ότι η ομαλή λειτουργία του Αερολιμένα εξαρτάται από την ομαλή λειτουργία του κέντρου επιχειρήσεων. Ως εκ τούτου πρέπει να διασφαλιστεί η ασφαλής πρόσβαση σε αυτό.

Ενόψει των δεδομένων αυτών και των αποφάσεων της Αρχής που προηγήθηκαν, η επεξεργασία βιομετρικών στοιχείων ίριδας των οφθαλμών, εξεταζόμενη υπό το πρίσμα των αρχών του σκοπού και της αναγκαιότητας, δεν αντίκειται σε διατάξεις του νόμου 2472/97 και συνεπώς επιτρέπεται η συλλογή και επεξεργασία των δεδομένων της ίριδας των οφθαλμών για την επαλήθευση της ταυτότητας των εργαζομένων που έχουν δικαίωμα πρόσβαση στο Κέντρο Επιχειρήσεων του Αερολιμένα. Και αυτό διότι ο σκοπός που επιδιώκεται με τη μέθοδο που προαναφέρθηκε είναι κρίσιμης και καθοριστικής σημασίας για τη διασφάλιση της ασφαλούς λειτουργίας του Αεροδρομίου και την προστασία των επιβατών και των εργαζομένων δεδομένου ότι ηπιότερα μέσα επαλήθευσης της ταυτότητας δεν χαρακτηρίζονται από τον ίδιο βαθμό ασφαλείας και αποτελεσματικότητας.

Για τους λόγους αυτούς:

Η επεξεργασία βιομετρικών στοιχείων για τη διασφάλιση της πρόσβασης των εργαζομένων του ΔΑΑ στο κρίσιμης σημασίας Κέντρο Επιχειρήσεών του (ΚΕΑ), η οποία γνωστοποιήθηκε με το με α.π. 2054, από 29-08-2003, έγγραφό του, είναι νόμιμη και συνεπώς επιτρέπεται η συλλογή και επεξεργασία των δεδομένων ίριδας

των οφθαλμών μόνον των εργαζομένων, οι οποίοι εισέρχονται και παρέχουν τις υπηρεσίες τους στο Κέντρο Επιχειρήσεων του Αερολιμένα.

Ελληνική Δημοκρατία. Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα
19/06/2007 Α.Π. 4422

Την καταγγελία του Σωματείου Εργατοϋπαλλήλων της εταιρείας Χ που δραστηριοποιείται στο χώρο των πλαστικών. Με την οποία καταγγέλθηκε η εγκατάσταση και λειτουργία βιομετρικού συστήματος ελέγχου της εισόδου και της εξόδου των εργαζομένων στο Β΄ υποκατάστημα της εταιρείας στη θέση Ζ περιοχής Β. Η Αρχή έχει κρίνει ότι η εισαγωγή και χρήση βιομετρικών μεθόδων συνιστά επεξεργασία προσωπικών δεδομένων εργαζομένων, η οποία δεν είναι αναγκαία για την επίτευξη των σκοπών του ελέγχου εισόδου και εξόδου σε εγκαταστάσεις / κτίρια και τήρησης του ωραρίου προσέλευσης και αποχώρησης τους και είναι, συνεπώς, παράνομη.

Ειδικότερα, η Αρχή έχει ήδη επιβάλλει, με την 245/9 (από 20/03/2000) Απόφασή της, την διακοπή της επεξεργασίας από Δήμο δεδομένων προσωπικού χαρακτήρα εργαζομένων του με τη μέθοδο της δακτυλοσκόπησης, για το σκοπό ελέγχου της εισόδου και της εξόδου από δημοτικό κτήριο, με το σκεπτικό ότι η μέθοδος αυτή υπερβαίνει το σκοπό της επεξεργασίας. Η Αρχή έκρινε, επιπλέον, ότι η υπέρβαση αυτή δεν αίρεται από τη συγκατάθεση των υποκειμένων και ότι πρέπει να επιλέγονται ηπιότεροι τρόποι για την άσκηση του εργοδοτικού ελέγχου. Επίσης, με ανάλογο σκεπτικό, η Αρχή απαγόρευσε, με την Απόφασή της 52/2003, την πιλοτική εφαρμογή βιομετρικού συστήματος στο αεροδρόμιο Ελευθέριος Βενιζέλος, το οποίο είχε σκοπό τη συλλογή και επεξεργασία δεδομένων δακτυλοσκόπησης και ίριδας του ματιού για την επαλήθευση της ταυτότητας των επιβατών, που επρόκειτο να ταξιδέψουν.

Αντίθετα, με την Απόφασή της 9/2003, η Αρχή, έκρινε – υιοθετώντας πάντως παρόμοιες σκέψεις – ότι δεν παραβιάζονται τα δικαιώματα των εργαζομένων, όπως αυτά κατοχυρώνονται ιδίως με την Οδηγία 115/2001, από την εγκατάσταση βιομετρικού συστήματος (στοιχεία της γεωμετρίας του χεριού), αποκλειστικά για το σκοπό του ελέγχου πρόσβασής τους σε ιδιαίτερα «ευαίσθητες» – από πλευράς ασφαλείας των συγκοινωνιών – εγκαταστάσεις του Αττικού Μετρό. Επίσης, με την Απόφαση της 39/2004, η Αρχή επέτρεψε, υπό προϋποθέσεις, τη συλλογή και

επεξεργασία των δεδομένων ίριδας των οφθαλμών μόνο των εργαζομένων που εισέρχονται και παρέχουν τις υπηρεσίες τους στο Κέντρο Επιχειρήσεων του Διεθνούς Αερολιμένα Αθηνών, με σκοπό τη διασφάλιση της πρόσβασης σε αυτό καθώς αποτελεί χώρο νευραλγικής σημασίας και ύψιστης ασφάλειας από την ομαλή λειτουργία του οποίου εξαρτάται η ομαλή λειτουργία του Αερολιμένα.

Εξάλλου, με ανάλογες σκέψεις, η Αρχή έκρινε, με την Απόφασή της 59/2005, ότι η επεξεργασία βιομετρικών στοιχείων φυσικών προσώπων για την πιλοτική εφαρμογή ερευνητικού προγράμματος δεν είναι νόμιμη και, συνεπώς, δεν επιτρέπεται η συλλογή και επεξεργασία δεδομένων δακτυλοσκόπησης για τον έλεγχο πρόσβασης φιλάθλων και διαπιστευμένων ατόμων σε αθλητικές εγκαταστάσεις. Τέλος, πάντα με ανάλογες σκέψεις, η Αρχή έκρινε πρόσφατα, με τις Πράξεις της 437/29-01-2007 και 1887/13-3-2007 ότι αντιβαίνει στις διατάξεις του Ν.2472/1997 και είναι, συνεπώς, παράνομη – ως δυσανάλογη, εν όψει του προβαλλόμενου σκοπού επεξεργασίας - η επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων Δήμου και Ταμείου αντίστοιχα, με την βιομετρική μέθοδο της δακτυλοσκόπησης για τον σκοπό του ελέγχου τήρησης του ωραρίου προσέλευσης και αποχώρησης των εργαζομένων.

Συνεπώς, η επεξεργασία των δεδομένων των εργαζομένων της καταγγελλομένης εταιρείας για τον έλεγχο της εισόδου και της εξόδου τους από τις εγκαταστάσεις της και τον έλεγχο τήρησης του ωραρίου προσέλευσης και αποχώρησής τους, με τη βιομετρική μέθοδο της ανάλυσης της γεωμετρίας του δακτύλου, είναι παράνομη.

Επειδή η καταγγελλόμενη εταιρεία προέβη σε παράνομη επεξεργασία των δεδομένων των εργαζομένων της. Επειδή παρέλειψε να γνωστοποιήσει στην Αρχή την συγκεκριμένη επεξεργασία, σύμφωνα με το άρθρο 6 του ν.2472/1997, μέχρι που της ζητήθηκε από την Αρχή, μετά την υποβολή της καταγγελίας του σωματείου των εργαζομένων της. Επειδή δεν παρείχε στην Αρχή τις ζητηθείσες πληροφορίες σχετικά με τα τεχνικά χαρακτηριστικά του βιομετρικού συστήματος, σύμφωνα με το άρθρο 19 παρ. 1 δε. η) του Ν.2472/1997. Επειδή δεν ενημέρωσε τους εργαζόμενους όπως προβλέπεται από το άρθρο 11 του Ν.2472/1997. Επειδή η εταιρεία είναι ζημιογόνος και ένα υψηλό πρόστιμο θα απέβαινε εξουθενωτικό για την περαιτέρω λειτουργία της. Για τους λόγους αυτούς:

Η Αρχή, διατάσσει την καταγγελλόμενη εταιρεία αμέσως να: α) διακόψει την συγκεκριμένη επεξεργασία, β) απεγκαταστήσει το βιομετρικό σύστημα που έχει

τοποθετήσει στις εγκαταστάσεις της, γ) καταστρέψει το αρχείο που έχει ήδη δημιουργήσει με τα δεδομένα των εργαζομένων της για τους παραπάνω σκοπούς και ειδικά τα βιομετρικά στοιχεία που τους αφορούν, σύμφωνα με τις επιταγές της οδηγίας 1/2005 της Αρχής περί ασφαλούς καταστροφής δεδομένων προσωπικού χαρακτήρα και δ) ενημερώσει σχετικά την Αρχή για τα παραπάνω.

Επιβάλλει στην καταγγελλόμενη εταιρεία πρόστιμο 1.500 ευρώ για τις παραβάσεις που αναφέρονται στο σκεπτικό της παρούσας.

Απευθύνει αυστηρή προειδοποίηση στην καταγγελλόμενη εταιρεία εφεξής να ενημερώνει τα υποκείμενα των δεδομένων σύμφωνα με το άρθρο 11 του Ν.2472/1997 και να γνωστοποιεί στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας σύμφωνα με το άρθρο 6 του ιδίου νόμου.

Ελληνική Δημοκρατία. Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα

22/09/2009 Α.Π. 5579

Με την υπ'αριθμ. πρωτ. 961/27-10-2008 αίτηση, η εταιρεία «ΑΝΤΑΚΟΜ Προηγμένες Εφαρμογές Διαδικτύου Ανώνυμος Εταιρεία» με έδρα την Αθήνα Αττικής γνωστοποίησε την χρήση βιομετρικών μεθόδων για τον έλεγχο της πρόσβασης σε συγκεκριμένα τμήματα του χώρου εργασίας της εταιρείας. Η ΑΝΤΑΚΟΜ ΑΕ αποτελεί πάροχο υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών και από το έτος 2002 είναι εγγεγραμμένη στο αντίστοιχο Μητρώο της ΕΕΤΤ ως «Πάροχος Υπηρεσιών Πιστοποίησης που εκδίδει Αναγνωρισμένα Πιστοποιητικά κατά δήλωσή του». Ως πάροχος υπηρεσιών πιστοποίησης αναγνωρισμένων πιστοποιητικών, η ΑΝΤΑΚΟΜ ΑΕ σε συμμόρφωση με την ισχύουσα νομοθεσία (Προεδρικό Διάταγμα 150/2001, «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές», Παράρτημα 2) υποχρεούται, μεταξύ άλλων, να χρησιμοποιεί αξιόπιστα συστήματα και προϊόντα που προστατεύονται έναντι τροποποίησης και να διασφαλίζει την τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης που υποστηρίζονται απ' αυτά. Μετά από σχετική μελέτη, η ΑΝΤΑΚΟΜ ΑΕ, λαμβάνοντας υπόψη την αρχή της αναλογικότητας, όπως αυτή προβλέπεται στο άρθρο 4 του Ν.2472/1997, και έχοντας εφαρμόσει αυστηρά μέτρα ασφάλειας, προχώρησε στην εγκατάσταση του συγκεκριμένου συστήματος σε ορισμένους μόνο χώρους εργασίας. Στους συγκεκριμένους χώρους της ΑΝΤΑΚΟΜ ΑΕ φυλάσσεται το κρυπτογραφικό υλικό (Ασφαλείς Κρυπτογραφικές Μονάδες), όπου

παράγονται και τηρούνται τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης τα οποία υπογράφουν τα Αναγνωρισμένα Πιστοποιητικά τελικών χρηστών. Η ΑΝΤΑΚΟΜ ΑΕ έχει διενεργήσει μελέτη Αποτίμησης Επικινδυνότητας των Πληροφοριακών Συστημάτων & Εγκαταστάσεων της (risk assessment) τα αποτελέσματα της οποίας αποκαλύπτουν την κρισιμότητα των Πληροφοριακών της Συστημάτων και την απαίτηση για ακεραιότητα και εμπιστευτικότητα των Ασφαλών Κρυπτογραφικών Μονάδων και των Ιδιωτικών Κλειδιών της Αρχής Εγγραφής και επομένως την ανάγκη εφαρμογής του συγκεκριμένου μέτρου ελέγχου. Τα συγκεκριμένα δεδομένα προσωπικού χαρακτήρα των υπαλλήλων που έχουν πρόσβαση στους χώρους αυτούς φυλάσσονται προς χρήση του βιομετρικού συστήματος για όσο χρόνο έχουν πρόσβαση στους χώρους αυτούς και μετά διαγράφονται. Επίσης, η εταιρεία ΑΝΤΑΚΟΜ ΑΕ προβαίνει σε αναλυτική ενημέρωση των υπαλλήλων σχετικά με την επεξεργασία των προσωπικών τους δεδομένα κατά το άρθρο 11 του Ν.2472/1997. Μετά από προφορική συνεννόηση της εισηγητού με στελέχη της ΑΝΤΑΚΟΜ ΑΕ στα γραφεία της Αρχής ζητήθηκαν συμπληρωματικά στοιχεία προκειμένου να εκτιμηθεί η αναγκαιότητα επιλογής του συγκεκριμένου μέτρου ασφαλείας. Τα στοιχεία αυτά, που κατατέθηκαν με την υπ'αριθμ. πρωτ. 1076/26-11-2008 αίτηση είναι τα ακόλουθα: α) Αποτίμηση Επικινδυνότητας, β) Πολιτική Ασφάλειας, γ) Απαιτήσεις Ελέγχου του Κέντρου Πιστοποίησης της VeriSign (απόσπασμα), δ) Τεχνική Περιγραφή Βιομετρικού Συστήματος, ε) Περιγραφή ρόλων για τους οποίους απαιτείται η χρήση βιομετρικών, στ)Σύμβαση Εχεμύθειας και Εμπιστευτικότητας (μεταξύ ΑΝΤΑΚΟΜ ΑΕ και του προσωπικού), ζ) Ενημέρωση και συγκατάθεση των υποκειμένων των δεδομένων (άρθρο 11 του Ν.2472/1997) και η) Τεχνικά φυλλάδια των βιομετρικών συσκευών. Ύστερα από μελέτη των παραπάνω στοιχείων διενεργήθηκε επιτόπιος έλεγχος στους συγκεκριμένου χώρους της ΑΝΤΑΚΟΜ ΑΕ με κύριο αντικείμενο τον έλεγχο λειτουργίας των συγκεκριμένων βιομετρικών συσκευών και τη διαπίστωση ότι οι προδιαγραφές ασφάλειας, όπως έχουν επισημανθεί από τη μελέτη επικινδυνότητας και την πολιτική ασφάλειας, έχουν εφαρμοστεί επακριβώς στους συγκεκριμένους χώρους.

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

Το άρθρο 2 του Νόμου 2472/1997, ορίζει ότι "δεδομένα προσωπικού χαρακτήρα" είναι " κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. «Υποκείμενο των δεδομένων» είναι, το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή

μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική. Από τις διατάξεις αυτές συνάγεται ότι τα δεδομένα που χρησιμοποιούνται για την ταυτοποίηση ενός προσώπου με χρήση βιομετρικών μεθόδων ή με άλλα λόγια η ψηφιακή απεικόνιση ενός φυσικού χαρακτηριστικού, αποτελούν προσωπικά δεδομένα. Επομένως, το προτεινόμενο σύστημα, όπως περιγράφεται ανωτέρω, εμπίπτει στην επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Τα δεδομένα προσωπικού χαρακτήρα πρέπει, κατά το άρθρο 4 της Νόμου 2472/1997, να συλλέγονται με τρόπο θεμιτό και νόμιμο, για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών. Επίσης τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας. Η παραπάνω αρχή του σκοπού προϋποθέτει τον σαφή προσδιορισμό του σκοπού για τον οποίο θα γίνει συλλογή και επεξεργασία των παραπάνω βιομετρικών δεδομένων. Δεν επιτρέπεται η επεξεργασία δεδομένων για άλλο σκοπό από εκείνον για τον οποίο εξαρχής έχουν συλλεγεί. Η αξιολόγηση των ζητημάτων της αναλογικότητας και της νομιμότητας εφαρμογής του σκοπού είναι απαραίτητη, λαμβάνοντας υπόψη τους κινδύνους που θέτει η χρήση των βιομετρικών τεχνολογιών σχετικά με την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών του ατόμου. Ειδικά για την επεξεργασία βιομετρικών δεδομένων η Αρχή Προστασίας Δεδομένων έχει ορίσει με την Οδηγία 112/2001, ότι ως νόμιμος σκοπός ορίζεται αυτός που αφορά την εφαρμογή ιδιαίτερων απαιτήσεων ασφάλειας των χώρων εργασίας λαμβάνοντας υπόψη ότι δεν υπάρχει άλλο μέσο για την επίτευξη του σκοπού αυτού. Ο υπεύθυνος της επεξεργασίας οφείλει, με τρόπο συστηματικό, να σταθμίζει από τη μια πλευρά την αναγκαιότητα εφαρμογής των βιομετρικών τεχνολογιών και από την άλλη τα δικαιώματα των εργαζομένων.

Στην προκειμένη περίπτωση, όπως αναφέρεται στην αίτηση του υπευθύνου της επεξεργασίας, αποκλειστικός σκοπός της επεξεργασίας είναι ο έλεγχος πρόσβασης σε εγκαταστάσεις υψηλών απαιτήσεων ασφάλειας. Ο αριθμός των υπαλλήλων που χρησιμοποιούν το υπό εξέταση σύστημα τελεί σε μια αναλογική σχέση προς το συνολικό αριθμό των εργαζομένων του υπευθύνου της επεξεργασίας και επίσης το βιομετρικό σύστημα αυτό καθεαυτό δεν υπερβαίνει την αρχή της αναλογικότητας καθώς τα δεδομένα αποθηκεύονται τοπικά σε κάθε συσκευή και όχι σε κεντρική βάση

με αποτέλεσμα να ελαχιστοποιείται ο κίνδυνος επεξεργασίας προσωπικών δεδομένων των υπαλλήλων σε περίπτωση αθέμιτης πρόσβασης από μη εξουσιοδοτημένα πρόσωπα. Ενόψει των παραπάνω παραδοχών, η Αρχή κρίνει, ότι το συγκεκριμένο σύστημα δεν αποτελεί σοβαρό κίνδυνο παραβίασης των προσωπικών δεδομένων των υπαλλήλων της αιτούσης εταιρείας, ενώ παραλλήλως δεν υπάρχει άλλο εξίσου αποτελεσματικό μέσο για την επίτευξη του υψηλού βαθμού ασφάλειας που απαιτεί η συγκεκριμένη δραστηριότητα αυτής και συνεπώς δεν αντίκειται στις διατάξεις του Ν.2472/1997 η εγκατάστασή του, με τους όρους που ορίζονται στο διατακτικό της απόφασης, για τον αποκλειστικό σκοπό του ελέγχου πρόσβασης ορισμένων εργαζομένων στους χώρους έκδοσης και επεξεργασίας ψηφιακών πιστοποιητικών. Η χρήση για άλλο σκοπό, όπως για παράδειγμα για την αξιολόγηση της συμπεριφοράς των εργαζομένων, απαγορεύεται.

Η τεχνολογία Υποδομής Δημοσίου Κλειδιού βασίζεται κυρίως στην παραδοχή της ακεραιότητας και εμπιστευτικότητας του κρυπτογραφικού υλικού και των ιδιωτικών κλειδιών των Αρχών Πιστοποίησης και επομένως η ΑΝΤΑΚΟΜ ΑΕ απαιτείται να εφαρμόζει τα κατάλληλα μέτρα ελέγχου για τη δέουσα φύλαξή τους. Η δυνατότητα πρόσβασης στο χώρο φύλαξης των κλειδιών μη εξουσιοδοτημένων προσώπων εγκυμονεί κίνδυνο παραβίασης των κλειδιών αυτών με σοβαρές συνέπειες τόσο για την ασφάλεια των συναλλαγών που στηρίζονται σε αυτά όσο και για την ΑΝΤΑΚΟΜ ΑΕ η οποία έχει εγγυηθεί στους δημόσιους και ιδιωτικού φορείς την μη παραβίασή τους. Σύμφωνα με το άρθρο 10 του Ν.2472/1997, η ΑΝΤΑΚΟΜ ΑΕ οφείλει να λάβει όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα ασφάλειας για την προστασία των προσωπικών δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Επομένως πρέπει να εφαρμοστούν κατά την επεξεργασία των βιομετρικών δεδομένων (αποθήκευση, μετάδοση, εξαγωγή χαρακτηριστικών και σύγκριση κλπ.) τα κατάλληλα μέτρα ασφαλείας.

Για τους λόγους αυτούς

Η Αρχή Προστασίας Δεδομένων κρίνει ότι η εγκατάσταση του παραπάνω βιομετρικού συστήματος αποκλειστικά για τον σκοπό του ελέγχου της πρόσβασης ορισμένων εργαζομένων στις συγκεκριμένες εγκαταστάσεις της εταιρείας ΑΝΤΑΚΟΜ ΑΕ δεν αντίκειται στις διατάξεις του Ν.2472/1997

Ηθική (Ethics)

Εγείρονται κάποια θέματα ηθικής όσον αφορά τη χρησιμοποίηση των βιομετρικών. Η συλλογή κάποιων βιομετρικών πληροφοριών όπως τα δακτυλικά αποτυπώματα, είναι συσχετισμένη με εγκληματίες στο μυαλό πολλών ανθρώπων. Παραδοσιακά, λεπτομερείς βιομετρικές πληροφορίες συγκεντρώνονται από μεγάλους οργανισμούς, όπως η αστυνομία και ο στρατός. Οι άνθρωποι ίσως νιώσουν ότι χάνεται η έννοια της ιδιωτικότητας και την προσωπικής αξιοπρέπειας. Αυτόματη αναγνώριση προσώπων σε δημόσια μέρη, μπορεί να χρησιμοποιηθεί έτσι ώστε κάποιος να παρακολουθείτε χωρίς να το ξέρει ή να έχει δώσει τη συγκατάθεσή του. Οι άνθρωποι νιώθουν ντροπή όταν σε ένα δημόσιο μέρος απορρίπτονται από έναν αναγνώστη (scanner). Επίσης όσον αφορά το γενετικό υλικό, κάποιες θρησκείες απαγορεύουν τη λήψη αίματος, καθώς και συστήματα που αναλύουν το γενετικό υλικό χρησιμοποιώντας ανθρώπινες τρίχες θα απέκλειαν τους ανθρώπους χωρίς μαλλιά.

Ανησυχίες επίσης υπάρχουν και με τον τρόπο αποθήκευσης των πληροφοριών και πού θα αποθηκεύονται. Δεν είναι δηλαδή κάποιες κάρτες που θα μπορούσαν να φυλάσσονται σε ένα ασφαλές κτήριο. Είναι ηλεκτρονικές πληροφορίες που εύκολα μεταφέρονται και αντιγράφονται. Επίσης ποιος θα έχει πρόσβαση σε αυτές τις πληροφορίες. Για παράδειγμα μεγάλες εταιρείες θα έχουν πρόσβαση σε βιομετρικά προσώπου, επιτρέποντας την αναγνώριση πελατών σε καταστήματα. Πως θα σας φαινόταν να μπαίνατε σε ένα πολυκατάστημα που δεν έχετε πάει ποτέ πιο πριν και ο πωλητής να σας υποδεχτεί γνωρίζοντας το μικρό σας όνομα, αφού πρώτα διαβάσει μια σύντομη περίληψη των στοιχείων σας και των τελευταίων αγορών σας;

ΣΥΜΠΕΡΑΣΜΑ

Τα Συστήματα Βιομετρική Αναγνώρισης σίγουρα θα διευκολύνουν πολύ στους τομείς που θα εφαρμοστούν, επιβολή του νόμου (law enforcement), έλεγχος φυσικής πρόσβασης (physical access control) συμπεριλαμβανομένου και του ελέγχου στα σύνορα και έλεγχος λογικής πρόσβασης (logical access control). Αποτελούν ένα κομμάτι της τεχνολογίας που αναπτύσσεται ραγδαία. Θα πρέπει να θεωρείται σχεδόν βέβαιο ότι σε λίγα χρόνια το ιδιαίτερα ευάλωτο τραπεζικό σύστημα των PINs, θα ενισχυθεί με ένα βιομετρικό σύστημα. Η συμμετοχή των βιομετρικών στην ασφάλεια στο διαδίκτυο θα είναι μεγάλη. Ο βασικός εξοπλισμός – μικρόφωνο για αναγνώριση φωνής και κάμερα για αναγνώριση γεωμετρίας προσώπου – ήδη υπάρχει στα περισσότερα υπολογιστικά συστήματα. Μένει μόνο να αναπτυχθεί η κατάλληλη υποδομή. Από οικονομικής πλευράς είναι σίγουρο ότι παρέχοντας μεγαλύτερα επίπεδα εμπιστοσύνης στους πελάτες θα ανθίσει το ηλεκτρονικό εμπόριο. Η υιοθέτηση των Βιομετρικών Τεχνολογιών από τις κυβερνήσεις είναι απαραίτητη. Μόλις οι πολίτες δουν ότι τα κυβερνητικά συστήματα είναι ασφαλή και εύχρηστα, οι ανησυχίες και οι προκαταλήψεις θα πάψουν να υφίστανται και έτσι θα διευκολυνθεί ακόμη περισσότερο η ηλεκτρονική διακυβέρνηση.

Παράλληλα όμως θα πρέπει να χρησιμοποιηθούν σωστά και να θεσπιστούν νόμοι για την εφαρμογή των βιομετρικών όσον αφορά την προστασία των δεδομένων των πολιτών. Κάθε εταιρεία ή οργανισμός θα πρέπει να λαμβάνει σοβαρά τους ανθρώπους οι οποίοι θα χρησιμοποιούν αυτές τις τεχνολογίες, χωρίς να προσβάλλει την προσωπικότητα και τη θρησκεία τους.

ΠΑΡΑΡΤΗΜΑ Α

Ερωτηματολόγιο

Γενικές Πληροφορίες

1)Φύλλο ερωτηθέντος: ☐Άντρας ☐ Γυναίκα

2)Ηλικία: ☐15-18 ☐19-27 ☐28-40 ☐41 και πάνω

3)Επάγγελμα ερωτηθέντος:
_____

Ειδικές Πληροφορίες

1)Πόσες φορές τη βδομάδα έχετε πρόσβαση σε ηλεκτρονικό υπολογιστή;
☐Καμία ☐ 1-3φορες ☐ 4-10φορες ☐10 φορές & πάνω

2)Για ποιο λόγο;
☐ Εργασία ☐ Ψυχαγωγία ☐ Ενημέρωση

3)Ποιες υπηρεσίες του Διαδικτύου χρησιμοποιείτε εσείς και η οικογένειά σας; (Διαβαθμίστε την κάθε επιλογή ανάλογα με τη χρήση της, από 1-9.

Καθόλου=1, Αρκετά=4, Πάρα πολύ=9)	**Εσείς**	**Ο / Η σύζυγος**	**Παιδιά**
Υπηρεσία e-mail			
Ανταλλαγή δεδομένων			
Υπηρεσία εικόνας			
Voice-over-IP			
Δικτυακά παιχνίδια			

4)Σε πόσες από της δραστηριότητες σας είναι αναγκαία η χρήση ενός password;

☐Σε καμία ☐1- 5 ☐6 και πάνω

5)Χρησιμοποιείται διαφορετικά passwords για κάθε υπηρεσία;

☐ ΝΑΙ ☐ ΟΧΙ ☐ Σε κάποιες

6)Πόσο εύκολα θυμάστε ένα password;
(Απαντήστε με ένα αριθμό από το 1 έως 9.
Ελάχιστα=1, Αρκετά=4, Πάρα πολύ=9)

☐ 1 ☐ 4 ☐ 9

7)Πιστεύετε πως τα passwords που χρησιμοποιείται είναι δύσκολο να "σπάσουν";
(Απαντήστε με ένα αριθμό από το 1 έως 9.
Ελάχιστα=1, Αρκετά=4, Πάρα πολύ=9)

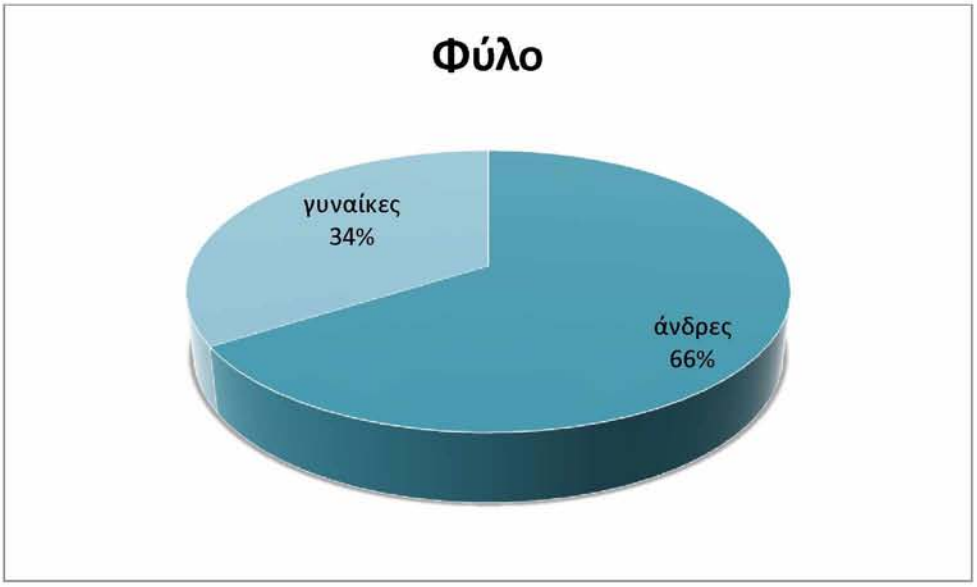
☐ 1 ☐ 4 ☐ 9

8)Έχετε κάπου γραμμένα τα passwords που χρησιμοποιείται συνήθως;

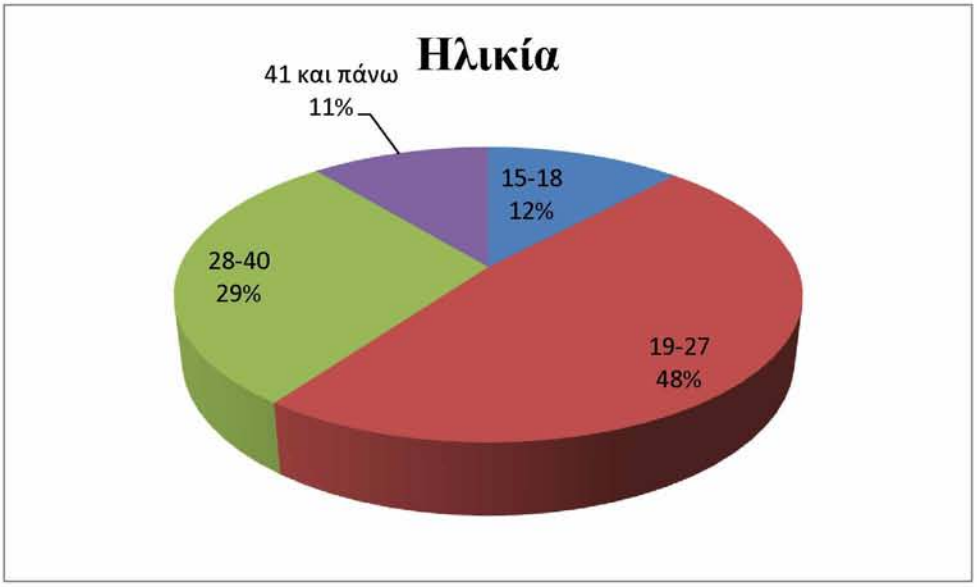
☐ ΝΑΙ ☐ ΟΧΙ

Ευχαριστούμε πολύ για το χρόνο σας

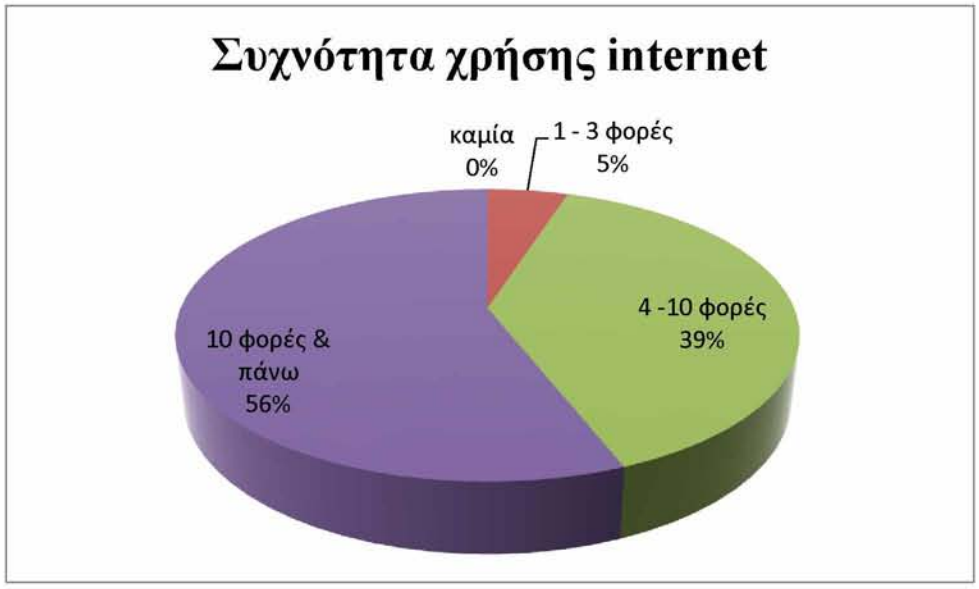
Αποτελέσματα έρευνας



Γράφημα 7.

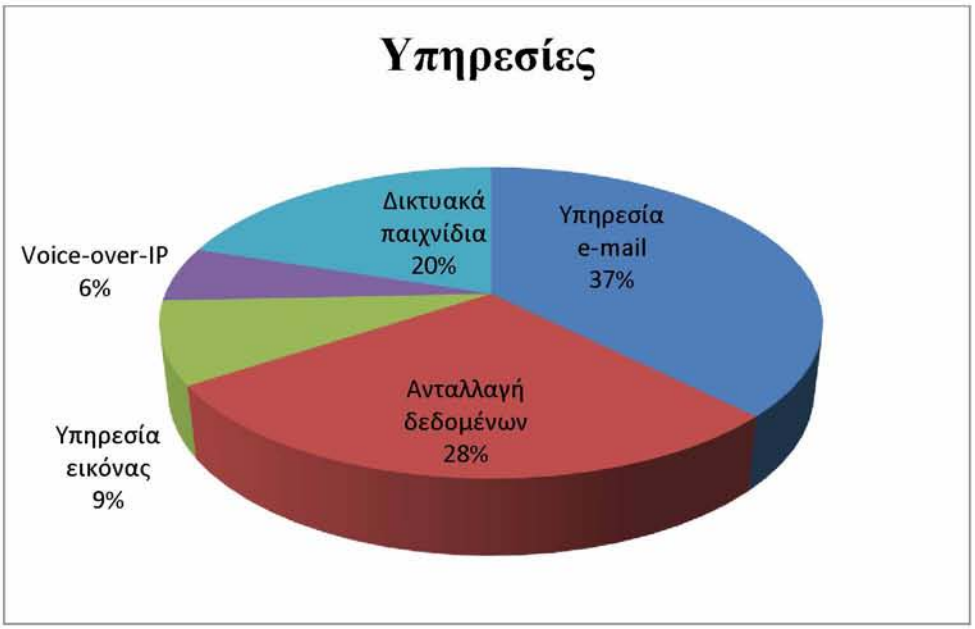


Γράφημα 8.



Γράφημα 9.

Γράφημα 10.



Γράφημα 11.

Γράφημα 12.

Γράφημα 13.

Γράφημα 14.

Γράφημα 15.

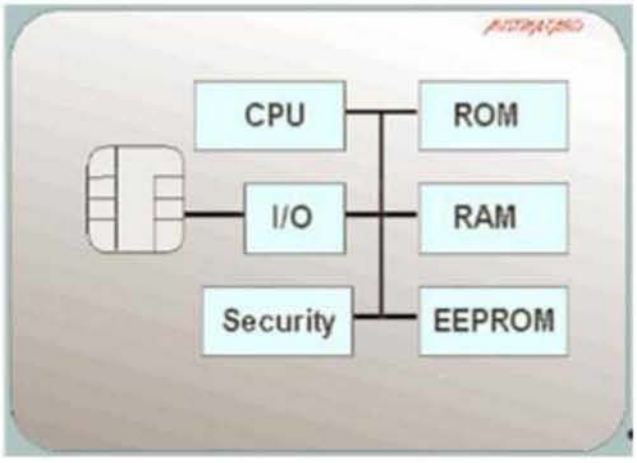
Γράφημα 16.

ΠΑΡΑΡΤΗΜΑ Β

Smart cards – Έξυπνες κάρτες

Μια smart card είναι μια κάρτα, κυρίως από πλαστικό (PVC), η οποία έχει ένα ενσωματωμένο ολοκληρωμένο κύκλωμα το οποίο μπορεί να επεξεργάζεται και να αποθηκεύει πληροφορίες. Ένας ενσωματωμένος μικροεπεξεργαστής ελέγχει τη λειτουργία των κύριων τμημάτων της κάρτας. Η RAM (μνήμη εργασίας) αξιοποιείται αποκλειστικά για προσωρινή αποθήκευση. Η ROM (μνήμη που δε διαγράφεται) αποθηκεύει το λειτουργικό σύστημα της κάρτας. Η EEPROM (μνήμη εφαρμογών) αποθηκεύει εφαρμογές και δεδομένα. Το μεγάλο μειονέκτημα αυτών των καρτών είναι ότι μπορεί να κλαπούν, να χαθούν ή να αντιγραφούν.

Εικόνα 50 και 51. Μια συνηθισμένη smart card. Μια smart card με ενσωματωμένο σύστημα αναγνώρισης δακτυλικού αποτυπώματος



Εικόνα 52. Το ολοκληρωμένο σύστημα μιας smart card

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]. Neath, I. Human memory: An introduction to research, data, and theory. Pacific Grove, CA: Brooks/Cole

[2]. Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1. Published as NIST Special Publication 500-271, May 2007

[3]. FBI Electronic Biometric Transmission Specification (EBTS) Version 8.1

[4]. Peter Gregory and Michael A.Simon. Wiley Publishing , Inc. Biometric for dummies

[5]. Fernando L. Podio and Jeffrey S. Dunn. Biometric Authentication Technology: From the Movies to Your Desktop

[6]. Sara Peters. 2009 CSI Computer Crime and Security Survey. Executive Summary

[7]. Dr. Eugene Schultz. Data Security Breaches: An Unstoppable Epidemic? March 2010

[8]. Jonathan Cave. Economic aspects of Biometrics. European Communities, 2005

[9]. Cave, J. (2005) "The economics of cyber trust between cyber partners" in R. Mansell and B. Collins (ed) Trust and Crime in Information Societies

[10]. InfoSecurity Europe. PriceWaterhouseCoopers. Information Security Breaches Survey 2010, Executive Summary

[11]. J. L. Wayman, "Technical Testing and Evaluation of Biometric Identification Devices", in Biometrics: Personal Identification in Networked Society. Kluwer Academic, December 1998

[12]. S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 8. August 2002

[13]. R. Derakhshani R, S.A.C. Schuckers, L. Hornak, L. O'Gorman, "Determination of Vitality From A Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners", Pattern Recognition, No.2. 2003

[14]. F. Podio, J. Dunn, L. Reinert, C. Tilton, Dr. L. O'Gorman, M. P. Collier, M. Jerde, Dr. B. Wirtz,Common Biometric Exchange File Format (CBEFF), NISTIR 6529, January 3 2000

[15]. Irman van der Ploeg. Biometric Identification Technologies: Ethical Implications of the Informatization of the Body. March 2005

[16]. Nora Rudon and Keith Inman. Principles and Practices of Forensic Science: The Profession of Forensic Science. 2002

[17]. Michael Lynch. God's signature: DNA profiling, the new gold standard in forensic science. June 2003

[18]. Dunn, Jeffrey S. and Fernando L. Podio. —Biometric Authentication Technology: From the Movies to Your Desktop. National Institute of Standards and Technology. National Security Agency. 2008

[19]. Carlos Busso, Zhigang Deng *, Serdar Yildirim, Murtaza Bulut, Chul Min Lee, Abe Kazemzadeh, Sungbok Lee, Ulrich Neumann*, Shrikanth Narayanan. Analysis of Emotion Recognition using Facial Expressions, Speech and Multimodal Information. 2004

[20]. Mase K. Recognition of facial expression from optical flow. IEICE Transc., E. 0ctober 1991

[21]. Pawan Sinha, Benjamin Balas, Yuri Ostrovsky, and Richard Russell. Face Recognition by Humans: Nineteen Results All Computer Vision Researchers Should Know About. IEEE, Vol. 94. 2006

[22]. Andrew Ryan, Jeffery F. Cohn, Simon Lucey, Jason Saragih, Patrick Lucey, & Fernando De la Torre, Adam Rossi. Automated Facial Expression Recognition System. IEEE 2009

[23]. Lee, H.C., Gaensslen, R.E.: Advances in Fingerprint Technology. 2nd edition, Elsevier, New York 2001

[24]. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition, Springer, New York 2003

[25]. Phillips, P.J., Moon, H., Rizvi, S.A., and Rauss, P.J. The FERET evaluation methodology for face- recognition algorithms. Trans. Pat. Anal. Mach. 2000

[26]. John Daugman. University of Cambridge. Iris Recognition for Personal Identification

[27]. Robert C. Yen. Forensic DNA Typing and Prospects for Biometrics. Department of Defense Biometrics Management Office. Summary Report, Biometric Identification Seminar, JUNE 2004

[28]. William C. Thompson, 1 J.D., Ph.D.; Franco Taroni,2,3 Ph.D.; and Colin G. G. Aitken,4 Ph.D. How the Probability of a False Positive Affects the Value of DNA evidence. J Forensic Sci, Jan. 2003

[29]. Sasse, A. Usability and trust in information systems. Report for the Cyber Trust & Crime Prevention Project, UK Office of Science and Technology Foresight Program. 2004

[30]. Ani K. Jain, Sharath Pankati, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman. Biometrics: A Grand Challenge. 2004

ΙΣΤΟΤΟΠΟΙ

http://www.dpa.gr

http://www.upek.com

http://www.safenet-inc.com

http://www.rsasecurity.com

http://www.gsmarena.com/first_gsm_with_vga_display__sharp_904-news-174.php

http://www.archives.gov

http://www.ibia.org

http://www.bioapi.org

http://biometrics.gov

http://www.foresight.gov.uk

http://www.tictac.gr/g-password.html

http://www.lock-center-hellas.gr/gr/company.php

http://www.manifest-services.gr/services.asp?pageID=252_223_258

http://www.biokey.gr/

http://www.keystamp.gr/